Delving

Journal of Technology and Engineering Science

ISSN 0975-5289
December 2019
Vol. 3 Issue 1

Articles

Acropolis Institute of Technology & Research Indore
www.acropolis.in

Journal of Technology and Engineering Science

ISSN 0975-5289

Editorial Office
Acropolis Delving
Department of Information Technology
Acropolis Institute of Technology & Research Indore
Bypass Road, Manglia Square, Manglia,
Indore, Madhya Pradesh – 453771
India

Integration of Blockchain with Internet of Things: A Literature Review

[1]Bhumika Sharma, [2]Krunali Sheth, [3]Shubhangi Sharma, [4]*Upendra Verma

[1,2,3,4]Department of Computer Science Engineering
Narsee Monjee Institute of Management Studies (NMIMS)
[1]bhumika.sharma44@nmims.edu.in,
[2]krunali.sheth47@nmims.edu.in,[3]shubhangi.sharma45@nmims.edu.i
n, [4]upendra.verma@nmims.edu.in

Abstract

Internet of Things (IoT) is a boundless network that interconnects anything and everything that we possess or operate within our daily life. It congregates an enormous amount of diverse information that assists in automating certain tasks. Due to the restriction of these IoT devices in storage, network capability and capacity, following challenges are to be considered and resolved: security, data privacy, robustness against cyber-attack, single point of failure and trouble-free authentication. In this paper, we have proposed the security of IoT using a decentralized and distributed network such as Blockchain. It is integrated with the IoT platform to provide efficient and transparent solutions to the problems mentioned above. by holding a motive to develop Blockchain-based IoT (BIoT) applications. This paper presents the basic idea about Blockchain and IoT concepts, highlights, and surveys about IoT security and how Blockchain can help in taking vital steps to solve security issues faced by various IoT platforms.

Keywords: Blockchain, IoT, Decentralization, Miners, Shared Ledger, Merkle Tree, Peer-to-Peer, BIoT

I. Introduction

Internet of Things (IoT) is about connecting various devices to the internet, and also to other devices that are present on the internet. IoT network is intensifying and some reports predict that IoT devices will grow to 26 billion by 2020[1]. These devices have inbuilt sensors that collect and flood us with a large amount of information, which is used to process further dependent activities. There is a wide range of smart connected devices or “things”, ranging from easy-to-wear gadgets to massive computers. Each one comes with sensor chips. But a significant drawback of IoT devices is that they are resource-constrained. Hence, they are not capable of performing massive processing and computations. They have issues of privacy, security, and incapability to protect them from getting hacked. All the valuable personal data of the user’s connected devices, revealing their behavior patterns, are directed to a central authority that can use it illegally [2]. Hackers can also break into the system and misuse the information. The author of [3] discloses that the user’s sensitive data managed by internet and telecommunication companies are put to wrong use under a mass surveillance program named as Prim’s Program. Prim’s is a tool used by NSA (US National Security Agency) to collect data of certain people from various companies such as Gmail, Facebook, Apple, Microsoft when having permission by the secretive Foreign Intelligence Surveillance Court.

The ineffectiveness of the IoT devices to perform heavy processing and computations are solved by utilizing fog nodes. Fog computing has come into view as a new computing model that has the potential of storing, processing, and analyzing data of a group of IoT devices. There is a demand for a user authentication scheme that is dependable, quantifiable, measurable, and rigid against threats and attacks [4]. Researchers perceive Blockchain technology as a distributed, decentralized system where the privacy and security of IoT devices are guaranteed. It was first used in Cryptocurrency transactions such as Bitcoin. This technology is not centralized; instead, it is a Peer to Peer (P2P) system where there is a shared ledger that keeps a record of each operation performed on IoT devices. As each operation is recorded, any mistreatment of data can be detected conveniently. Blockchain is capable of providing solutions to all the problems and challenges faced by the IoT system. It can track and store data from a large number of devices, making them connectable and functional without a centralized cloud system.

In the present scenario, IoT systems are operating with a centralized system that has complications, such as the centralized clouds are expensive to deploy and maintain. They are difficult to maintain, as an updated version of software needs to be distributed to all the devices in the network. [5]

IoT device users are having trouble trusting technology partners, who, in particular, allow certain officials to have access and supervision of devices. Governments, producers, or service providers are the ones who enable user data gathering and analysis.
Transparent approaches must be taken into account in the development of the next generation of IoT solutions to boost confidence and security.

The combination of a P2P storage system and the Blockchain could promote a private-by-design IoT. Crucial data generated and shared between IoT devices are stored in a storage system whose P2P existence ensures confidentiality, robustness and the omission of the single failure point. In combination with this storage scheme, the Blockchain plays a fundamental role in registering and authenticating all IoT device information activities. The Blockchain can specify and enforce access policies to prevent unauthorized information activities. In this context, individuals are not obliged to entrust centralized enterprises for information generated by their devices. Rather pieces of information are stored securely in distinct peers, and a blockchain may ensure authentication and avoid unauthorized access.

As reported in [6], Venture capital investments in blockchain startups increased from US$ 93 million to US$ 550 million from 2013 to 2016. In addition, the global blockchain technology market is projected to expand to US$ 2.3 billion by 2021.Consequently, Blockchain’s main input is that it offers a way of conducting transactions with another individual or entity without relying on third parties. Thanks to numerous decentralized miners who monitor and validate each transaction.

This paper discusses the basics of Blockchain, smart contracts, and provides a good survey about the challenges faced by current IoT devices and suggests the integration of Blockchain with IoT as a solution. Our research aims at understanding whether the Blockchain and, in general, P2P approaches can foster a private-by-design IoT, where the data of IoT devices belongs to the device owner, who decides which data is shared and with whom. Hence, the data of the IoT devices is not entrusted to centralized companies.

II. Problem Formulation

A. Blockchain

Being a decentralized, distributed, shared, and unchangeable database ledger, Blockchain stores assets and transaction records across the peer-to-peer (P2P) network. Each transaction in the directory is digitally signed and validated through tens of thousands of network mining nodes.[7]
In the Blockchain, the third party people are replaced by miners, who study and validate every transaction and then helps to add the new block in the Blockchain. Transactions in groups known as blocks are stored and structured by time stamps. These blocks are bound together into a blockchain or a chain of blocks. Block size is approximately 1 MB on average. The container data structure containing a sequence of transactions is the structure of a block. Block in the context of Bitcoin has two components, one is block header, and the other one is a transaction list. The Block header consists of the prior block hash, which is then used to build the present block hash, then the mining statistics and the Merkle root that builds stores all of the transactions, or a hash value which is there. Block transactions are structured as a Merkle tree whose Merkle root is used to build a hash block. If you alter a transaction, all the following block hash needs to be altered. Merkle trees definitely play their part in the efficient and secure storage of information. A hash tree is the Merkle tree's alternative name. It is a tree data structure whose leaf nodes hold hash of the document, and each individual and intermediate node shall contain the hash of the combination of the left child under a right child. The root hash of the Merkle tree is called Merkle root, which ensures that none of the documents has been changed. Figure 1 shows the structure of the Block and Merkle tree of Blockchain.
A block is valid if it includes valid transactions and if miners have conducted a computationally hard puzzle that consists of discovering a lower-than-predefined target hash of the block. The miner adding the next block to the Blockchain is the first to have a valid block assembled and discovered a valid alternative to the puzzle. This particular method of mining is called Proof-of-Work (PoW). The PoW enables us to reach distributed consensus, which implies that all nodes agree on the same blockchain version, and this Blockchain includes valid transactions.
The nodes in the network often cannot reach unanimous consensus on the future state of the Blockchain due to which Forks occur in the Blockchain, that is, the perfect 'single' Blockchain is divided into two or more valid chains. The rule for the forks is that miners stretch the longest or the most challenging branch to the PoW. Furthermore, due to PoW, it is difficult to tamper Blockchain.

There is a long-time financial problem called Double Spending. In this, there is a risk of spending the digital currency twice, which can be done easily on the internet rather than physical currency by the people who master the computation used in the blockchain network by copying the transaction details and reusing them.

This problem is solved by Blockchain by a consensus algorithm called Proof-of-Work (PoW). Miners prevent double-spending and maintain the accuracy of the previous transactions. [8]
In a P2P network, each network node gets two keys: a public key that is used by the other customers for encryption and a private key that decrypt messages sent by customers. The documents encrypted with the respective public key can only be decrypted with the appropriate private key. It is known as asymmetric encryption. The Blockchain utilizes elliptic curve cryptography (ECC) and SHA2 (Secure Hash Algorithm Two) hashing system to provide powerful cryptographic evidence for

authentication and integrity of information. To sign transactions, the Elliptic Curve Digital Signature Algorithm (ECDSA) is used by the Bitcoin and Ethereum. ECC is a public-key encryption technique based on a finite graph's algebraic feature and curve structure. ECC and other digital signature systems using trapdoor features stay some of the world's safest techniques of encryption. A series of hash functions are used to produce our public key and create a distinctive address. SHA256 is the basis of the hashing function. A 64 hexadecimal string of letters and numbers will result from any data set entered into the SHA256 function. If an input is given, you can use the hash function to generate an output. However, it is not possible to reconstruct its input using the output of the hash function. This strong characteristic of the hash function SHA-256 makes it perfect for use. It is used for two purposes within the Bitcoin network which are mining and Bitcoin Address Creation.

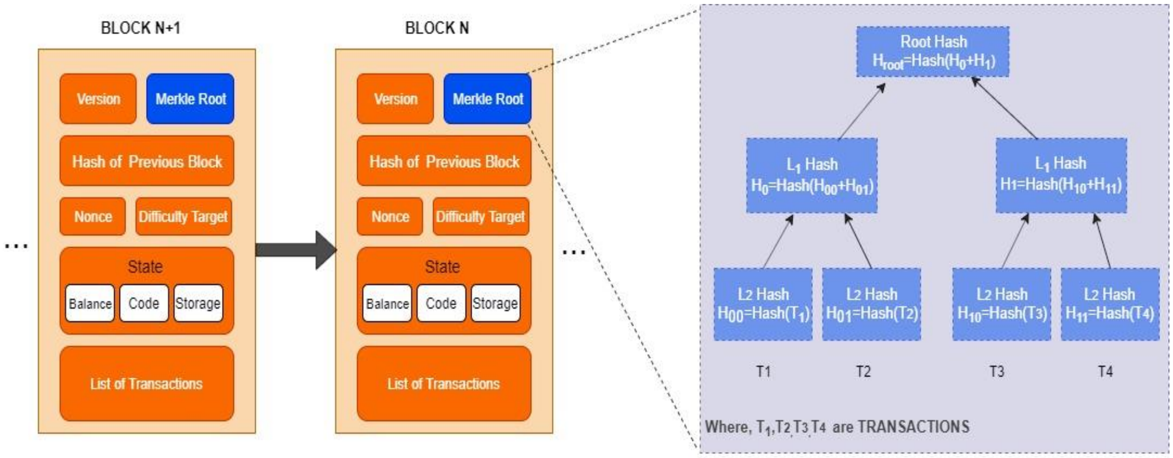


Fig. 1. Blockchain Framework of Chained Blocks [11]

B. Types of Blockchain

"Blockchain" technology has been launched into the globe by Bitcoin.
We all are aware that it all began in 2008 with the whitepaper of Satoshi Nakamoto, and in 2009, the first Bitcoin was mined. Depending on the data being managed, the availability, and what actions a user can do, there are different types of blockchains. It can be differentiated between public and private, permissioned, and permission less Blockchain. In government blockchains, anyone can join the Blockchain, acting as a simple node or miner without a third party's consent. Different decentralized consensus processes such as Proof of Work (PoW) and Proof of stake (PoS) are used for decision-making, etc. In public blockchains such as Bitcoin, Ethereum, or Litecoin, miners are generally provided financial incentives. [9] In private Blockchain, the owner limits access to the network. In order to regulate which customers can conduct transactions, execute smart contracts, or behave as miners in the network, many private blockchains are permissioned. Examples of permissioned blockchains are those used by Hyperledger Fabric or Ripple. [10] There is one more type of Blockchain called Consortium or Federated Blockchain. In this, you have more than one in charge instead of one. Basically, a group of businesses or representatives is coming together to make choices that will benefit the entire network to the greatest possible degree. These groups are also known as consortiums or federation. To determine whether the use of a blockchain is suitable, a

developer should decide whether an IoT application requires the following characteristics:

a) Decentralization - IoT apps require decentralization if a trusted centralized system is not in place. However, a blockchain is not needed if there is mutual confidence.
b) *P2P* - Most of the IoT communications go from nodes or gateways to a remote server or internet.
c) *Payment system* - Some IoT-application implementations can include economic transactions with third parties, but many apps do not. In contrast, traditional payment methods are still essential for economic transactions.

“Fig.2” shows a standard flow diagram which helps to determine the type of blockchain required based on the IoT system's characteristics.

C. Biot Applications

Blockchain evolution started from Blockchain (1.0) i.e. Bitcoin where the transacted value on the network is cryptocurrency. Then we evolved to Blockchain (2.0) where the transacted value is programmable transactions known as Smart Contracts. In 1994 Nick Szabo introduced the term smart contracts for the first time. In fact, [11] a smart contract is a computerized transaction procedure to satisfy contract terms. There are stored program in these contracts which gets executed as soon as the required conditions are met, therefore also called as self-executing, decentralized contracts which are immutable. In order to create smart contracts, Solidity is the scripting and programming language that is like the JavaScript code. Ethereum Blockchain includes EVM (Ethereum Virtual Machines) that are essentially the miner nodes. Such nodes are capable of providing trustworthy implementation and compliance of these services and agreements. Applications of smart contracts are Supply Chain Management, Mortgage Loans, employment contracts, etc. Ethereum is the platform on which smart contracts are created. It is an open-source, public, blockchain-based distributed computing platform and operating system. Later, it moved to Blockchain (3.0), which is an upgraded version of Blockchain (2.0) having an objective to solve scalability problems and making cost-effective, efficient and less time-consuming transactions.
They are a vast range of applications of Biot such as Sensing [12], Government and democracy [13], Telecommunications [14], Information Systems [15] [16], Transportation [17], smart objects [18], Healthcare [19], Industry 4.0 [20].
For IoT agricultural applications, blockchain can also be used. For example, a traceability framework for the monitoring of Chinese food supplies has been presented in [21]. The RFID and blockchain networks are used to enhance food security and efficiency and to reduce distribution delays.

It is also possible to benefit the energy sector by applying a blockchain to IoT or the Energy Internet (IoE) [22] [23]. A blockchain network allowing IoT / IoE systems to charge each other for goods without human intervention. A system's future implementation: a smart cable connected to an intelligent socket is payable for used energy. In Healthcare BIoT applications, the framework of the clinical trial and precision medicine blockchain-based platform is introduced. The work mentioned in [24] proposed a broad-based smart health system using IoT tools, cloud and fog computing [25].

Other BIoT applications include Smart House. The basis of building a Smart house using the integration of IoT and Blockchain has three tiers, namely: cloud storage, overlay, and smart home. IoT bids for a lightweight, scalable and distributed security and privacy safeguards.Blockchain technology has the potential to overcome the above mentioned challenges due to its distributed, secure, and private nature.
Blockchain consists of miners that centrally manage smart devices present in the smart home tier. The overlay network introduces the distributed feature to the architecture. A cluster of nodes in the overlay is formed, where each cluster elects a cluster head. This decreases network overhead and delay. These Cluster Heads maintains a Blockchain in concurrence with Requester Key List (list of overlay users) and Public Key Lists so as to store data and access the cloud storage devices generate Store Transactions and Access Transactions, respectively. The shared key employed with Lightweight Hashing secures the communication as well as helps to detect any changes in transaction contents. The smart home devices are symmetrically encrypted. The storage of all the transactions is done in the local private blockchain. To store and share data, the smart home devices utilizes Cloud Storage. The time-ordered history of the transaction once appended in the ledger cannot be mutated later. The essential element of building a smart house is communication between local devices and overlay nodes, that is, transactions.

For devices that need to communicate directly, one solution could be that the miner allots them a shared key. For this, owner permission is appealed. Once the devices receive the shared key, they can communicate until their key is valid. The following are the benefits of this method: a) the miner or the owner has a list of devices that share data, b) the security of communication among devices is provided by a shared key.

A shared overlay is defined to lower the cost and manage overhead when more than one home is included. Although individual miners and storage are needed for each house, a shared miner manages them centrally as a single home. The simulation results in this paper demonstrate that the overheads incurred by their method are low and manageable for low resource IoT devices. If these overheads seem to be worth their weights given, the significant security and privacy benefits on offer [26] [27].

D. Challenges faced by IoT architecture

The most prominent factor to be considered when it comes to data transfer and its handling is Security.

Data Privacy and Integrity:

The architecture of IoT consists of the integration of several devices, networks, and nodes in that network. Thus, the confidentiality of data is a necessity as it travels through multiple routers or intermediate points. A poor encryption mechanism may lead to malicious attacks, which can affect the integrity of the data.

Three A's:
1) Authentication comes into play when there is a communication between two alliances. Certain privileges to access services must be provided to an authenticated person only [11]. The challenge

is to define a standard global protocol for authentication in IoT.
2) Authorization is to make sure that the system and data are accessed only by authorized parties. Integrating authentication and authorization results in a strong and secure communication environment.
3) Accounting is keeping records of resources used, audits and reports.

Quality-of-Service:
Different procedures, including the sinkhole attacks, jamming adversaries, etc. misuse IoT components at various layers to crumble the nature of administration (QoS) being given to IoT clients.

Energy Utilization:
The IoT gadgets are generally asset compelled and are described by low power and less stockpiling. The assaults on IoT structures may bring about an expansion in energy utilization by flooding the system and depleting IoT assets through repetitive or fashioned service requests. [11]

In terms of IoT implementation design, security threats are categorized as defined below:

- Low-level security issues
- Intermediate-level security issues
- High-level security issues

Low-level security issues
The first level of security tackles security problems both at the physical layer, data link layer and in the hardware layer, jamming the rivals. [28**]** [29]. The jamming of IoT wireless devices is aimed at network degradation or unsafe activation by transmitting radios frequency signals without using a specific protocol. A safe framework to enable and customize IoT on the physical layer assures that the entire system functions properly without compromising the confidentiality or disturbance of network services [30] [31].

Sleep deprivation attack
In IoT, the energy-restricted sensors are vulnerable to attacks of “sleep deprivation” by forcing the sensor nodes to remain awake [32].
When a large number of tasks are scheduled to be executed in the 6LoWPAN setting, battery depletion occurs.

Intermediate-level security issues -
Here, the focus is on the interaction. Routing and session control of IoT networks and transport layers are as listed below:

- Replay or duplication attacks due to fragmentation [11]
- Insecure neighbor discovery
- Buffer reservation attack
- Session establishment and resumption Privacy violation on cloud-based IoT

High-level security issues:

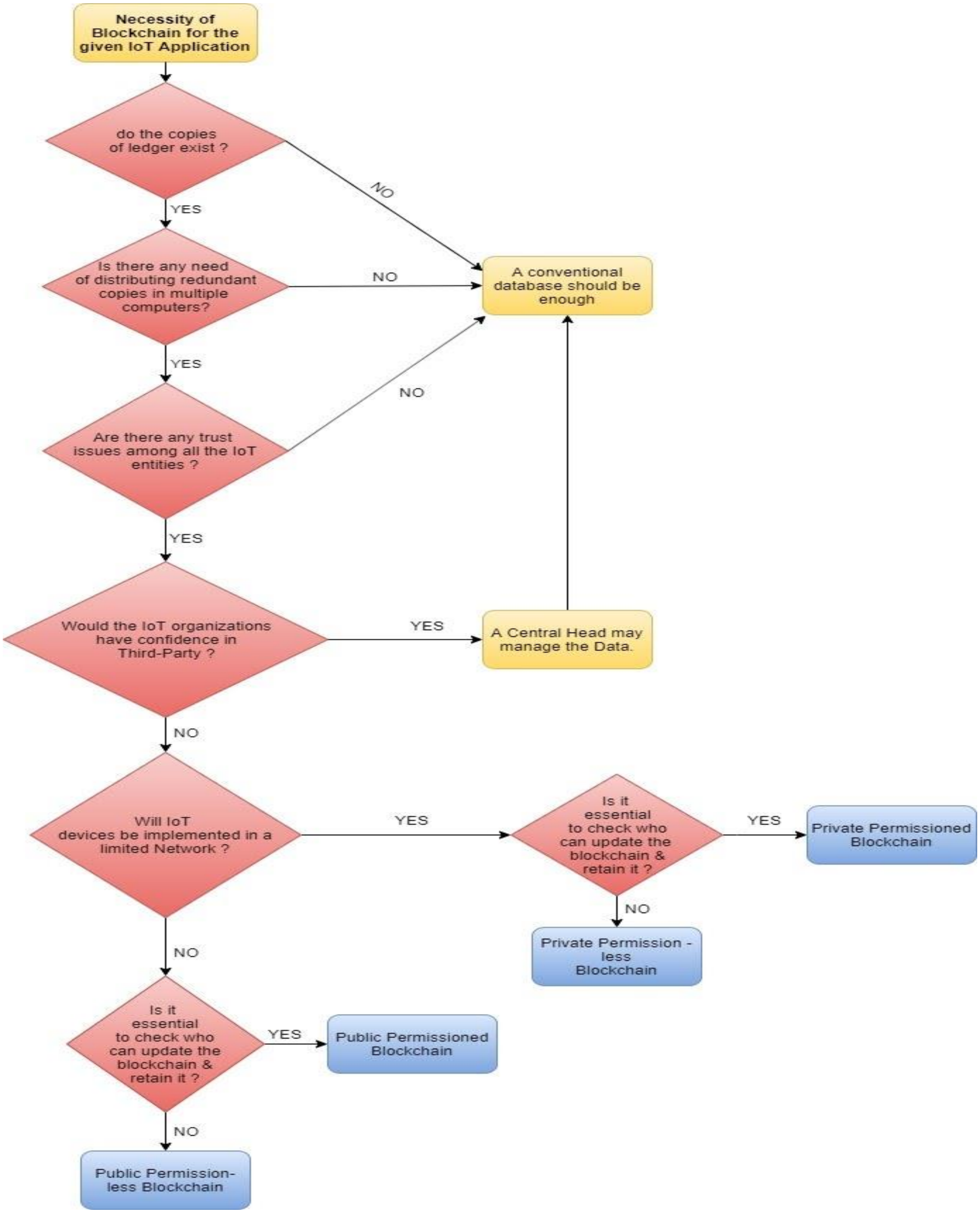

Necessity of Blockchain for the given IoT Application
do the copies of ledger exist ?
NO
YES
Is there any need of distributing redundant copies in multiple computers?
NO
A conventional database should be enough
YES
NO
Are there any trust issues among all the IoT entities ?
YES
Would the IoT organizations have confidence in Third-Party ?
YES
A Central Head may manage the Data.
NO
Will IoT devices be implemented in a limited Network ?
YES
Is it essential to check who can update the blockchain & retain it ?
YES
Private Permissioned Blockchain
NO
Private Permission - less Blockchain
NO
Is it essential to check who can update the blockchain & retain it ?
YES
Public Permissioned Blockchain
NO
Public Permission-less Blockchain

Fig. 2. Flow chart to determine when an IoT application requires Blockchain and of which type[8]

The high-level security concerns are primarily related to IoT as listed below:

- CoAP security with internet Insecure interfaces
- Insecure software/firmware
- Middleware security

The constant development of heterogeneous systems for the IoT based framework may uncover an enormous number of single-points of-failure, which may thusly crumble the services visioned through IoT. It requires the improvement of a carefully designed environment for an enormous number of IoT devices.

E. Blockchain as a solution

Blockchain innovation has been anticipated by industry and research networks as a problematic innovation that is ready to assume a noteworthy job in overseeing, controlling, and generally significantly verifying IoT gadgets. This area portrays how blockchain can be a key empowering innovation for giving feasible security answers for today's challenging IoT security issues. This segment first gives a concise foundation about blockchain and after that, blueprints IoT security issues and difficulties which blockchain may give answers for. The segment likewise reviews the writing of blockchain-based solutions for IoT security issues.

This leverages public key cryptography: each individual is identified by a public key and the law provides limited access to the relevant entities' public keys. Only the data holder has full access to its details. Policies are placed in blockchain, and blockchain nodes are tested for adherence.
We should further examine the safety properties of the PoW, which, up to now, is one of the key factors allowing a decentralized agreement to be reached.

In the world of technology and digitalization, reduced man work and security are the main aspects to be attained. IoT and Blockchain are the technologies that will improve efficiencies, provide new business opportunities, address regulatory requirements, and improve transparency and visibility. IoT makes provisions for real-time data from sensors. Blockchain makes it easier to share key relevant data provided by IoT via distributed, decentralized, shared ledger.
As for supply chain solutions, IoT and Blockchain together have solved real business problems, wherein, IoT devices attached to the products emit key shipment data and the IoT platform invokes a transaction. These transactions are captured by blockchain that contains the shipment container location and timestamp, and serves as a proof of shipment.
In manufacturing plants, IoT sensors can be used to detect critical and hazardous conditions which might lead to failures or injuries. The role of blockchain is to capture the key threshold data and report the trends of failures and expedite the required maintenance and repairs beforehand. Smart vehicles that would automatically pay for replenishments without direct human involvement could demonstrate that IoT with Blockchain could bring the industrial sector a business value. Vehicle sensors emit data to the IoT platform such as fueling, charging, parking, and repair events. The IoT platform invokes the appropriate blockchain transaction based on rules tied to the type of received sensor data. An open API integration layer is used by these facilities to invoke a transaction on the blockchain when the operation is complete [32] .
The concoction of IoT and Blockchain, despite these implications, can boost up the Industrial

Growth.

The most relevant vulnerabilities of current IoT systems, based on the cloud is that the entire system ceases running when the server is down due to cyber threats, repairs and software issues. If a single IoT computer is hacked, it can interrupt the entire network by initiating Denial of Service (DoS) attacks
[33], searching private data [34], modifying the information collected [35] or misleading other systems [36].
Edge and Fog Computing can be used to enable mobile, low-latency and QoS-Aware devices to reduce network and device congestion in conventional cloud computing networks.
“Fig. 3” depicts the conceptual scenario of BIoT. [37], BIoT architecture is proposed. The researchers model a lightweight conceptual architecture with safety and privacy in mind in these articles, which reduces overhead interactions in a blockchain. The system is designed for home automation.

Various components of the BIoT architecture are described below -

1) Sensors – They come in the device connectivity layer. They collect data from the environment and pass it on to the next layer. Type of sensors – temperature, pressure, humidity, moisture sensors, RFID tags, and light intensity detectors.

2) Device Connectivity – today’s’ smart devices and sensors are connected by low power wireless networks such as Wi-Fi, ZigBee, Bluetooth, Z-wave, LoRaWAN .

3) LoRa-
LoRa Technology is IoT DNA that connects sensors to the cloud and allows information and analysis to be communicated in real-time, which can be used to increase effectiveness and productivity.

4) Z-wave - Z-Wave is a protocol for wireless communications used mainly for home automation. It is a network of networks with low-energy radio waves that allow for wireless control of residential and other appliances.

5) Gateway - is a dedicated hardware device or software program connected between devices/sensors and cloud for bidirectional data transfer. It pre-treats the data, reduces the quantity of the data by reviewing it which in turn reduces the response time and network communication cost. Devices in Gateway- a) PIR sensor; b) Arduino UNO; c) Raspberry Pi gateway d) LED; e) IBM Watson IOT Platform.

6) Cloud- all the data generated from devices, applications, users, and websites is collected, stored, processed, managed and analyzed by the tools in the cloud. It is a network of sensors that provides a huge amount of data to business companies to analyze and make their business strategy.

7) Analytics - data received from billions of sensors and smart devices is used for real-time analysis, improvement and management of the irregularities in the stored data or system.

8) User Interface - is a platform where the user interacts with the system. A user-friendly and interactive design requires less effort from the user and insists them to buy such devices.

Components of Blockchain:

• *Node and Node Application* - every user or a pc that is a part of the architecture is called as node. This node must have a node application which helps it to connect to the network.

• *Block* - container data structure contains a series of transactions. The average size of the block is around 1MB.

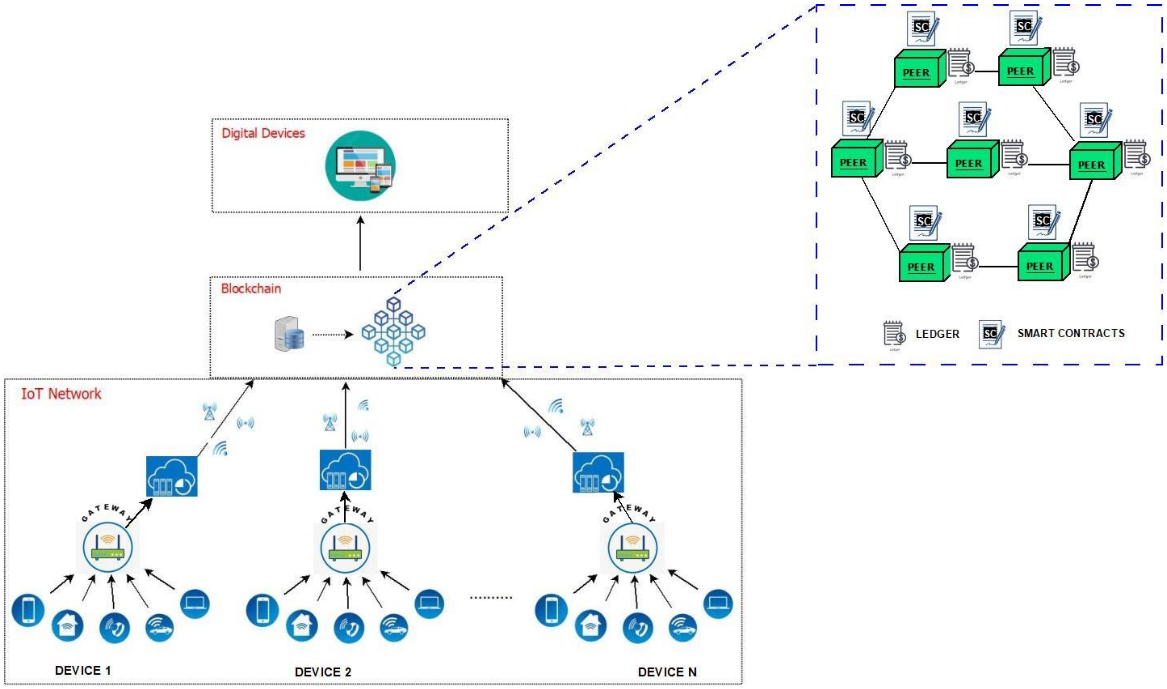


Fig. 3. Conceptual Scenario of BIoT

Structure of the Block:
a) Header – has previous block hash, Merkle tree root, mining statistics used to create the block.
b) List of transactions – they are organized as a Merkle tree and are difficult to change because if a single transaction is changed, the transactions performed before will have to be changed as well.

• *Shared Ledger* – it is like a record file that contains all records from the start till the end. Every node in the Blockchain has a copy of the ledger. It has to be consistent.

• *Consensus* – a set of rules that ensures every node has the most updated and similar copy of the public ledger.

• *Miners* – are just nodes who perform the specific task of adding a new block in the chain by proving it to be valid. For that, they have to compute complex mathematical problems, and the solution is called Proof of Work (PoW). PoW proves that a lot of resources and time is spent on solving the problem.In BIoT, centralized server is replaced with decentralized Blockchain system. It should be able to handle the traffic generated by IoT devices. Figure 3 shows the integrated architecture of Blockchain and IoT.

F. Drawbacks of blockchain

Integrity -

The biggest risk to the credibility of the blockchain is the existence of misbehaving miners who possess a large share of the system's computational power.

The key idea behind mixing protocols is that a client transmits coins to another address so that it is difficult to detect communication between the user's input and output addresses.

This could result in the formation of forks in blockchain, contributing to a scenario where it is challenging to achieve shared consensus and some prior information may be destroyed. It is dangerous to begin a totally new blockchain that in the initial phase has no critical mass.

The safest approach is to build IoT implementations on top of an existing secure blockchain, where PoW and a large number of trustworthy miners guarantee transparency and discourage misbehaving miners from obtaining a large share of computational power.

Anonymity -

The fair exchange protocol mentioned in [41] is also focused on the same concept of mixing protocols and permits the safe exchange of money between the two parties.

The authors of [42] concluded that to achieve complete secrecy, pseudonimism is not enough. Solutions that reduce the ability of IoT systems to be connected to their operators should be explored further in future work.

Adaptability –

There is a problem of scalability in the blockchain. The first is that the blockchain grows in size when the amount of transactions rises, and it becomes costly to store it, particularly for IoT devices with finite resources. The decentralized design in which the blockchain is isolated from the application layer may address this issue. IoT users with limited resources also store the component of the ledger they use for their own transactions.

The second problem is the poor transaction efficiency, a standard Bitcoin blockchain concern. The poor quality is induced by the PoW complexity and a total size of 1 MB of a frame. With respect to the PoW, if its complexity is lowered, the performance will be lower, but at the same time, it will be easier for an intruder to trigger blockchain forks.

To end, the Bitcoin blockchain scalability problems make it unsuitable for IoT, so we recommend the creation of IoT software in addition to another stable or scalable blockchain.

III. Literature Review

Title of Paper And Year of Publishing	Authors	Objectives and Contents	Technologies used	Research gap
Survey on blockchain for Internet of Things **2019**	Xu Wang, Xuan Zha, Wei Ni, RenPing Liu, Y. Jay Guo, XinxinNiu, Kangfeng Zheng	A comprehensive survey on existing Blockchain technologies with an emphasis on the IoT applications; potential adaptations elaborated on the Blockchain consensus protocols and data structures.	Blockchain; Internet of Things (IoT); consensus protocol; data structure.	effective integration of Blockchain into the IoT networks.
Blockchain mechanism for IoT security **2018**	Daniel Minoli, Benedict Occhiogrosso	IoT CPS Blockchains Security Integrity e-health ITS Consensus algorithms Blockchain applications; some IoT environments where Blockchain mechanisms(BCMs) play an important role, while at the same time pointing out that BCMs are only part of the IoT Security (IoTSec) solution.	IoT; CPS; Blockchains; Security Integrity; e-health; ITS; Consensus algorithms; Blockchain applications.	need for comprehensive support of security in the IoT, especially for Mission-critical applications, but also for the down-stream business applications.
Blockchain and the Internet of Things in the Industrial Sector **2018**	Dennis Miller	how these two technologies will improve efficiencies, provide new business opportunities, address regulatory requirements, and improve transparency and visibility; how the Blockchain will enable the sharing of key relevant data captured from the IoT using a distributed, decentralized, shared ledger that is available to participants in the business network.	Maintenance Engineering; Industrial Engineering; Internet Of Things; Supply Chains; Blockchain Technology.	need of address regulatory, legal, and insurance requirements for goods transferred on the supply chain, autonomous vehicles, and manufacturing plant equipment; close monitoring of safety records and test results by regulators, insurance adjusters, and legal institutions; access to safety records and equipment failure data needed by Law Firms for litigation.
A User Authentication Scheme of	Randa Almadhun, Maha Kadadha, Maya	a user authentication scheme using blockchain-enabled fog nodes in which fog nodes interface to	Fog Computing; Cloud Computing; Ethereum	potential threats and attacks on the overall system(like Confidentiality requirement, Integrity and

IOT Devices using Blockchain-enabled Fog Nodes **2018**	Alhemeiri, Maryam Alshehhi, Khaled Salah	Ethereum smart contracts to authenticate users to access IoT devices; Description system components, architecture and design; discussing key aspects related to security analysis, functionality, testing and implementation of the smart contracts.		non-repudiation).
A Review on the Use of Blockchain for the Internet of Things **2018**	Tiago M. Fernandez-Carames, Paula Fragalamas	how to adapt blockchain to the specific needs of IoT in order to develop Blockchain-based IoT (BIoT)applications; How blockchain can impact traditional cloud-centered IoT applications.	distributed systems, BIoT, fog computing , edge computing	Complex technical challenges (scalability, security, cryptographic development, etc); lack of centralized approaches; Interoperability and standardization; a comprehensive trust Blockchain framework; Rapid field testing

The Self-Driving Car Timeline – Predictions from the Top 11 Global Automakers
2017
	J. Walker	5 different levels of autonomy:
		Level 0-2- here, Human Driver Monitors Driving Environment.
		Level 3-5- here, Automated Driving System Monitors Driving Environment.
		Level 0- No Automation
		Level 1- Driver assistance
		Level 2- Partial automation
		Level 3- Conditional automation
		Level 4- High automation
		Level 5- Full automation
			Automation and Robotics;
			Artificial Intelligence;
			Transportation;
			Research and Development.
				Right legal and technical structures required for autonomous vehicles;
				Serious liability concerns when machines operate themselves in a potentially dangerous environment.

Cognitive radio based internet of things: Applications, architectures, spectrum related functionalities, and future research directions 2017	A.A.Khan, M.H. Rehmani, A.Rachedi	survey architectures and frameworks of CR-based IoT systems; discussion of spectrum-related functionalities for CR-based IoT systems and open issues, research challenges, and future direction for these CR-based IoT networks.	Internet of Things, Energy consumption Sensors, Cognitive radio, Machine-to-machine communications, Wireless sensor networks, Network	Challenges affecting the design of a CR-WSN: 1. Detection, False Alarm, and Miss- Detection Probability 2. Hardware; 3. Topology Changes 4. Fault Tolerance 5. Manufacturing Costs 6. Clustering 7. Channel Selection

			architecture cognitive radio capability CR-based IoT systems spectrum-related functionalities	8. Power Consumption 9. Quality of Service (QoS) 10. Sensing Techniques

Blockchain for IoT Security and Privacy: The Case Study of a Smart Home
2017
	Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram	a lightweight instantiation of a BC particularly geared for use in IoT by eliminating the Proof of Work (POW) and the concept of coins; Three main tiers in smart home setting: 1.cloud storage 2.overlay 3.smart home; an always online, high resource device, known as ”miner”, responsible for handling all communication within and external to the home, also preserves a private and secure BC, used for controlling and auditing communications.	Transactions;
			Local Blockchain;
			Home Miner;
				Results are quite encouraging; this research is the first work that aims to optimize BC in the context of smart homes.

IoTsecurity:Review, blockchain solutions, and open challenges 2017	Minhaj Ahmad Khan, Prof. KhaledSalah	mapping of the major security issues for IoT to possible solutions tabulated; Blockchain technology and its robust solutions for challenging and critical IoT security problems reviewed; parametric analysis of	- Diverse Networks with Gateways - Wireless sensor network with Gateways - Home appliances - Cyber Physical	Resource limitations; Heterogeneous devices; Interoperability of security protocols; Single points of failure; Trusted updates and management; Blockchain vulnerabilities.

		the state-of-the-art IoT security issues and solutions described.	Systems (CPS)	

Blockchain for the Internet of Things: a Systematic Literature Review
2016
	Marco Conoscenti, Antonio Vetro, Juan Carlos De Martin	whether the blockchain and Peer-to-Peer approaches can be employed to foster a decentralized and private-by-design IoT;18 use cases of blockchain; issues in the integrity, anonymity and adaptability	IoT;
			Peer-to-Peer (P2P) systems;
			Mining Attacks(selfish, stubborn);
			De-Anonymization Techniques; PKI or time stamping.
				address the integrity and the adaptability issues;
				testing existing secure and scalable blockchains;
				designing a layered architecture for IoT applications best suited; to achieve anonymity and further protect people’s privacy.

Blockchain beyond bitcoin
2016
	S. Underwood	a brief history of blockchain;
		identifying some of the key features that have enabled its popular uptake in the world of cryptocurrencies;
		how blockchain technologies have evolved from traditional software and web technologies;
		Examine their underlying strengths and evaluate new, non-cryptocurrency use cases.
			Blockchain;
			Smart contracts;
			Distributed ledger;
			Bitcoin;
			Cryptocurrency.
				Complexity as Blockchain technology involves an entirely new vocabulary;
				Network Size;
				Transaction Costs, Network Speed;
				Human Error;
				Unavoidable Security Flaw; Politics

Home automation system based on intelligent transducer Enablers
2016
	M. Suárez-Albela, P. Fraga-Lamas, T. M. Fernández-Caramés, A. Dapena, and M. González-López	a novel home automation system named HASITE (Home Automation System based on Intelligent Transducer Enablers), specifically designed to identify and configure transducers easily and quickly and simplifies the deployment of a home automation system.	home automation;
			IoT; plug-and-play;
			wireless sensor networks;
			transducer;
			self-configuration;
			ISO/IEC/IEEE 21451
				The results were encouraging; no such gap was observed.

Bitcoin and beyond: A technical survey on decentralized digital currencies 2016	F. Tschorsch and B. Scheuermann	structuring the many fold results and research directions; introducing the Bitcoin protocol and its building blocks; exploring the design space by discussing existing contributions and results; insights at the core of the Bitcoin protocol and its applications.	Bitcoins, cryptocurrency	Bitcoin becoming a point of manipulation for cyber thieves; various attacks(from packet sniffing to the double spending, etc.) effective security solutions to ensure proper functioning of Bitcoin in the future are still absent; issue of user privacy and anonymity.
Saving the Future of the Internet of Things 2015	Device Democracy	Why today's Internet of billions of Things won't scale to the Internet of hundreds of billions of Things: Broken business models, High cost, Lack of privacy, Not future proof, Lack of functional Value Pyramid of digital success: 1. Design rule Create better products and experiences 2. Business model guidelines. Prepare for new Digital economies, Create collaborative value. 3.Technology principles Design for peer-to-peer systems, Design for trustless communication, Design for decentralized autonomy.	Closed and centralized IoT networks, Open access IoT networks, Centralized cloud, Distributed cloud	Allowing technologies to control us; Unemployment and disturbance.
Internet of things: Security vulnerabilities and challenges 2015	Andrea, C. Chrysostmou, G.Hadjichritofi	exploring the security aims and goals of IoT and then provides a new classification of different types of attacks and countermeasures on security and privacy; future security directions	Security analytics (collecting, correlating, and analyzing data from multiple sources); Public Key	IoT becoming embroiled in controversy related to security issues. The most common security threats involve hijacking, leaks, unsecured devices and even home intrusion.

	Infrastructure (PKI); Network Security (anti-malware, antivirus, intrusion prevention, and firewalls); Device Authentication	

IV. Conclusion

Our study was comprised of the survey regarding the Internet of Things and its unification with Blockchain to resolve numerous data security concerns in IoT, even though IoT is an emerging topic of technical, social, and economic significance. Customary objects are being combined with Internet connectivity and robust data analytic capabilities, and yet IoT raises significant challenges in the way of realizing its potential benefits. We investigated the uses cases of the Blockchain in the literature and which factors affect integrity, anonymity, and adaptability of this technology. Regarding integrity and adaptability, we found that the most secure are large blockchain systems such as Bitcoin. At the same time, IoT is Ideal for Bicoin scalability problems. Concerning anonymity in the Blockchain, only guarantees pseudonymity. Our future work will be to test existing secure and blockchains for integrity and adaptability issues, as well as to develop a layered IoT architecture on top of the most appropriate. Moreover, we will investigate solutions to achieve anonymity and further protect people's privacy. The Blockchain technologies were analyzed in detail, followed by the applicability of the comparable technologies to the IoT scenarios. By merging these streams, we offered a substantial vision to improve the capacity, security, and scalability of Blockchains for future effective integration of Blockchain and IoT technologies.

References

[1] Forecast: The Internet of Things, Worldwide, 2013, Gartner, Stamford, CA, USA, Nov. 2013.

[2] Marco Conoscenti, Antonio Vetro, Juan Carlos De Martin, "Blockchain for the Internet of Things: a Systematic Literature Review", IEEE,2016.

[3] "NSA Prism program taps into user data of Apple, Google and others," http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[4] M. A. Khan and K. Salah, "IoT security: Review, Blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395 – 411, 2018. [Online]. Available: http://www.sciencedirect. com/science/article/pii/S0167739X17315765.

[5] S. Landau, "Making sense from Snowden: What's significant in the NSA surveillance revelations," IEEE Security Privacy, vol. 11, no. 4, pp. 54–63, Jul. 2013.

[6] Markets and Markets; Statista Estimates. Market for Blockchain Technology Worldwide.

Accessed: Apr. 10, 2018. [Online]. Available: https://www.statista.com/statistics/647231/worldwide-blockchaintechnology-market-size.

[7] Marco Conoscenti, Antonio Vetro, Juan Carlos De Martin, "Blockchain for the Internet of Things: a Systematic Literature Review", IEEE,2016.

[8] TIAGO M. FERNÁNDEZ-CARAMÉS, PAULA FRAGA-LAMAS," A Review on the Use of Blockchain for the Internet of Things", IEEE,Vol. 6, MAY 2018.

[9] Litecoins. Accessed: Apr. 10, 2018. [Online]. Available: https:// litecoin.com.

[10]Hyperledger-Fabric. Accessed: Apr. 10, 2018. [Online]. Available: https://www.hyperledger.org/projects/fabric

[11] Minhaj Ahmad Khan, Khaled Salah,"IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, NOV. 2017.

[12] D. Wörner and T. von Bomhard, ''When your sensor earns money: Exchanging data for cash with Bitcoin,'' in Proc. UbiComp Adjunct, Seattle, WA, USA, Sep. 2014, pp. 295–298.

[13] A. Wright and F. P. De. (Mar. 2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Accessed: Apr. 10, 2018. [Online]. Available: https://ssrn.com/abstract=2580664.

[14] A. Wright and F. P. De. (Mar. 2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Accessed: Apr. 10, 2018. [Online]. Available: https://ssrn.com/abstract=2580664.

[15] S. Wilkinson et al. Storj a Peer-to-Peer Cloud Storage Network. Accessed: Apr. 10, 2018. [Online]. Available: https://storj.io/storj.pdf.

[16] G. Ateniese, M. T. Goodrich, V. Lekakis, C. Papamanthou, E. Paraskevas, and R. Tamassia, ''Accountable storage,'' in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., Kanazawa, Japan, Jul. 2017, pp. 623–644.

[17] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, ''Blockchain-based dynamic key management for heterogeneous intelligent transportation systems,'' IEEE Internet Things J., vol. 4, no. 6, pp. 1832–1843, Dec. 2017 .

[18] M. Samaniego and R. Deters, ''Internet of smart things-IoST: Using blockchain and CLIPS to make things autonomous,'' in Proc. IEEE Int. Conf. Cogn. Comput. (ICCC), Honolulu, HI, USA, Jun. 2017, pp. 9–16.

[19] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, ''Blockchains everywhere—A use-case of blockchains in the pharma supply-chain,'' in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM), Lisbon, Portugal, May 2017, pp. 772–777.

[20] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, ''Blockchain technology innovations,'' in Proc. IEEE Technol., Eng. Manage. Conf. (TEMSCON), Santa Clara, CA, USA, Jun. 2017, pp. 137–141.

[21] F. Tian, ''An agri-food supply chain traceability system for China based on RFID & blockchain technology,'' in Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM), Kunming, China, Jun. 2016, pp. 1–6.

[22] Y. R. Kafle, K. Mahmud, S. Morsalin, and G. E. Town, ''Towards an internet of energy,'' in Proc. IEEE Int. Conf. Power Syst. Technol. (POWERCON), Wollongong, NSW, Australia, Sep./Oct. 2016, pp. 1–6

[23] T. M. Fernández-Caramés, ''An intelligent power outlet system for the smart home of the Internet of Things,'' Int. J. Distrib. Sens. Netw., vol. 11, no. 11, p. 214805, 2015, doi: 10.1155/2015/214805.

[24] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, ''Softwarization of

Internet of Things infrastructure for secure and smart healthcare,'' Computer, vol. 50, no. 7, pp. 74–79, Jul. 2017.

[25] K. Dolui and S. K. Datta, ''Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing,'' in Proc. Global Internet Things Summit (GIoTS), Geneva, Switzerland, Jun. 2017, pp. 1–6.

[26] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home ", ResearchGate Conference Paper, MAR. 2017.

[27] "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home " IEEE Percom Workshop On Security Privacy And Trust In The Internet Of Thing. March 2017

[28] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. http://dx.doi.org/ 10.1145/1062689.1062697

[29] G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30.

[30] S.H. Chae, W. Choi, J.H. Lee, T.Q.S. Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans. Info. for. Sec. 9 (10) (2014) 1617–1628.

[31] Y.-W.P. Hong, P.-C. Lan, C.-C.J. Kuo, Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches, IEEE Signal Process. Mag. 30 (5) (2013) 29–40.

[32] Dennis Miller,"Blockchain and the Internet of Things in the Industrial Sector", IEEE Computer Society, MAY 2018

[33]T. Bhattasali, R. Chaki, A survey of recent intrusion detection systems for wireless sensor network, in: D.C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, D. Nagamalai (Eds.), Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280

[34] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, ''Use of honeypots for mitigating DoS attacks targeted on IoT networks,'' in Proc. Int. Conf. Comput., Commun. Signal Process. (ICCCSP), Chennai, India, Jan. 2017, pp. 1–4.

[35] Q. Xu, P. Ren, H. Song, and Q. Du, ''Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations,'' IEEE Access, vol. 4, pp. 2840–2853, 2016

[36] X. Li, H. Wang, Y. Yu, and C. Qian, ''An IoT data communication framework for authenticity and integrity,'' in Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI), Pittsburgh, USA, Apr. 2017, pp. 159–170

[37] T. Yu, X. Wang, and A. Shami, ''Recursive principal component analysisbased data outlier detection and sensor data aggregation in IoT systems,'' IEEE Internet Things J., vol. 4, no. 6, pp. 2207–2216, Dec. 2017

Authors

Bhumika Sharma, Computer Engineering Student, Narsee Monjee Institute of Management Studies (NMIMS).

Krunali Sheth, Computer Engineering Student, Narsee Monjee Institute of Management Studies (NMIMS).

Shubhangi Sharma, Computer Engineering Student, Narsee Monjee Institute of Management Studies (NMIMS).

Upendra Verma obtained his Master of Engineering (Computer Science and Engineering) in 2011 at Rajiv Gandhi Technological University, Bhopal, India. He is working as Assistant Professor in NMIMS University. His research interest include Internet of Things, Network Security, Fog Computing and Authentication techniques

An Efficient Algorithm for High Utility Pattern Mining from Transactional Databases

[1*]Ritumbara Chauhan, [2]Kalyani Tiwari
[1,2]Computer Engineering, Indore Institute of Science and Technology India
[1]ritumbarachauhan25gmail.com, [2]kalyaniupadhyay86@gmail.com

Abstract

Main purpose of data mining is to find useful data set from raw data. Various data mining techniques are present. One of them is Frequent Pattern Mining technique which was used for find frequent patterns from databases. For usefulness of such frequent patterns, many constraints had been proposed by many researchers like utility parameters (price, profit, quantity etc.) as well as weight of an itemset etc. Mining high utility patterns from transaction database mainly focuses on the utility value of an itemset. Many algorithms have been proposed for finding user's goal previously, but they contain some limitations for large datasets when number of candidates itemsets are large. And when we talk about number of itemset when large number of candidates itemsets are present as raw data, it degraded the performance of the algorithm in the terms of memory requirement and execution time. The most significant problem of utility mining is that these patterns do not satisfy anti-monotonicity property and hence mining high utility patterns using traditional association rule mining algorithm becomes difficult. Additionally, when long transaction is considered the situation become worse. In this paper, we present a survey and comparison among various association rule mining algorithms which deals with high utility patterns mining are considered.

Keyword: Data Mining, Assoiciation Rule Mining, Interestingness Measure, Utility Mining.

I. Introduction

1.1 Data Mining

Data mining is also known as knowledge discovery in database. It established a prominent and research area in recent years. The main goal of data mining is to mine useful data or we can also use information from the raw data. It has been used in different different domain. Algorithmic process in which ouptut is generated for the respective input, in the data mining same as algorithmic process input are taken in the form of dataset and output is generated in the form of High utility patterns.

1.2 Association Rule Mining

To apply Association Rules Mining and get rules from transactional databases is one of the research problems in data mining when the itemset share framework. For finding frequent patterns and rules among the itemset Association Rule Mining is the best algorithm. From the transaction dataset, itemset which have support more than minimum support were found and rules with confidence having confidence more than user defined threshold are found as frequent patterns. In

these algorithms various data structure is used. When the number of transaction dataset are increases then it also increases its complexity, many newer data structure and algorithms are being developed to match this development. Association Rule Mining process consist two steps. In first steps, from the dataset all frequent itemsets are found and in second step association rules with respect to the frequent patterns are generated.

1.3 Utility Mining

Utility Mining is shown as a new development in data mining technology. A pattern is of utility if it helps him in decision making. It is referring to allow a user to express his or her perspective concerning the usefulness and utility of patterns and at last find the patterns which have utility value higher than a user defined threshold. Utilities of patterns are used to describe the user's goal; it is described by utility-based measures. Utility can be classified into two categories as follows:

a) Transaction Utility: It is the value or information which is directly from the transaction dataset e.g.Weight asso- ciated with the item.

b) External Utility: It is the utility which is given by the user, it is based on user interest for e.g. profit associated with item.

Normally the utility is defined as:

$$UOI = EU(e) * IU(e) \tag{1}$$

Where UOI stands for Utility of itemsets, EU(e) stands for External Utility and IU(e) stands for Internal Utility.

1.4 Interestingness Measure

Interestingness measure [6] can play an important role in Utility Mining for fulfilling the user's goals. It depends on the utility (usefulness) of the item sets.

Interestingness Measure can be classified into three categories as follows:

a) Objective Measure: It is mainly based only on the raw data. In it, user's knowledge and application knowledge is not required. Most of these measures are based on the theories in statistics, probability or information theory. For e.g. Apriori Algorithm considers only numbers and occurrence.

b) Subjective Measure: It is mainly based on both the data and users of these data. User's domain is required in these measures along with the background knowledge about the data. This can be accessed by interacting with the user or by understanding the user's goals. For e.g. Utility Mining.

c) Semantic Measure: It considers the explanations as well as semantics of the patterns. Because It involves domain knowledge from the user hence researcher sometimes considers it as a special type of subjective measures.

II. Problem Statement

2.1 Utility Mining Problem

There is a transaction database D is given. Along with the dataset minimum utility threshold *min utility"* is also given here, the main objective is to discover all the item sets which have high-utility. Let us consider the example database shown in Table 4.1 and in Table 4.2 the profit is given with respect to the transaction dataset. In the transaction dataset, each value indicates the quantity sold for an item. The support and confidence calculated in table 4.3 using internal utility given in table 4.1 and external utility given in table 4.2.

Table 3 Table for Comparison Between Support and Profit

Item sets	Support	Profit
P	90	120
Q	60	800
R	80	1178
S	90	91
PQ	60	885
PR	70	495
PS	80	166
QR	60	1142
QS	60	850
RS	60	392
PQR	60	1227
PQS	60	935
PRS	60	477
QRS	60	1192
PQRS	60	1277

Another example shows that no anti-monotonicity prop- erties is not satisfied in utility mining problem in which itemsets share framework. Let us consider an another trans- actional database shown in Table 4.4 and external utility table shown in Table 4.5.

Table 4 Transactional Table

Transaction ID	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**
Tr1	2	0	2	0	2	0	**0**
Tr2	7	3	3	0	0	6	**0**
Tr3	2	2	2	3	7	0	**6**
Tr4	4	2	0	5	4	0	**0**
Tr5	**3**	**2**	**0**	**3**	**0**	**3**	**0**

Table 1. Transactional Table

Transaction ID	**Item P**	**Item Q**	**Item R**	**Item S**
Tr1	4	0	1	**0**
Tr2	2	0	0	**6**
Tr3	0	0	21	**30**
Tr4	3	0	0	**5**
Tr5	2	1	1	**7**
Tr6	5	1	3	**11**
Tr7	3	1	1	**2**
Tr8	2	2	2	**9**
Tr9	1	2	1	**11**
Tr10	**6**	**1**	**1**	**10**

Table 4.4 shows the transactional dataset in which weight is given respect to the given item for various transactions. Table 4.5 presents the profit corresponds to the given itemset in Table 4.4.

Table 2. Profit Table

Item Name	**Profit**
Item P	**5**
Item Q	**100**
Item R	**38**
Item S	**1**

Profit here represents the external utility measures which have been discussed in section 3.
If the minimum support is taken 40% , it can be observed that the frequent itemsets in Table 4.3 are S, P, PS, and R, but the four most profitable itemsets are PQRS, PQR, R, and RS, all of which are infrequent itemsets. Therefore it is not necessary that the itemsets which have high support also have high utility.

Table 5. Profit Table

Item Name	**Profit**
I1	3
I2	5
I3	7
I4	4
I5	4
I6	3
I7	3

An itemset is high utility itemset or here represented by HUPSet which have utility value less than the predefined minimum threshold value. High Utility Patterns are generated are shown below: HUPset = $I1, I2, I4,\ I1, I2, I4,\ I1, I4, I5,\ I1, I2, I4, I5,\ I2, I3, I4,\ I3, I4,\ I1, I2, I3, I4, I5, I7$. Here HUPset stands for High Utility patterns itemset. It can be observed that pattern is not anti-monotone, because subsets of the frequent patterns are also frequent but in the case of utility it is fail. Anti-monotonicity property is not applied for utility mining so it is a new approach for high utility pattern mining is proposed.

III. Related Work Done

A. **Apriori Algorithm**

Agrawal et al. [1] propose an algorithm which is based on frequent pattern and also known as frequent pattern mining algorithm, named as Apriori Algorithm where target was found in second phase. In it, support measure is considered. The support is used for finding the finding the frequent pat- terns. If support measures of candidates are greater than minimum threshold value then the itemset are frequent patterns. for mining frequent patterns, It is a very famous breadth-first algorithm, which scans the disk-resident database as many times as the maximum length of frequent patterns. However, disadvantage of this popular algorithm is that it assumes transaction database are memory resident and it requires numerous database scans which increase time and space complexities. Anti-monotonicity property does not hold in Transaction dataset when we talk about share framework, fro resolving this problem Tao et al. [1] proposed a new concept of weighted closure property. Although weighted association rules mining considers the importance of items, in some application such as transaction databases items quantities in transaction are not considered.

B. Two Phase Algorithm

Ying Liu et al. [2] proposed a new algorithm for the same objective that discovering high utility patterns. Algorithm named as Two Phase Generation Algorithm. Two steps are presents in the proposed algorithm. It finds the high utility pattern in the first phase and scan the data one or more time to identify the high utility pattern in second phase. The main shortcoming of this approach is that when the number of candidates is increasing, the algorithm becomes inefficient in terms of space requirement.

C. Isolated Item Discarding Strategy (IDS)

To overcome memory insufficiency problems in Two Phase Algorithm a new algorithm was proposed by Lie et al. [4] for the same aim named Isolated Item Discarding Strategy (IDS). It is mainly proposed for the reduce the number of candidates generated in the first phase of Two-Phase Algorithm. By pruning isolated item sets for HTWUIS (High Transaction Weighted Utilities) in first phase, it can be reduced. Due to several database scan time, it takes more time. And after it, using the candidate and test scheme to discover the high utility item sets but still it also becomes inefficient in time.

D. IHUP Tree Algorithm

To efficiently generate high transaction weighted utilities in first phase and avoid database scan time, Ahmed et al. [8] has proposed a new algorithm based on a tree data structure. It is named as Tree I-HUP Algorithm, same as the name, these algorithms are based on the tree-based data structure. Information about item sets and their utility is maintained by these data structure. I-HUP Tree consist nodes, which consist of an item name and transaction weighted support count and utility value with it. This algorithm contains three steps. First is the I-HUP tree construction, second step is to generate the high transaction weighted utilities and third is identification of high utility item sets. With compare to IDES and Two-Phase candidate generation algorithm, THUP- Tree algorithm achieves better performance. But still too many high utility transaction weighted itemset are generated by this algorithm in phase one. Such a large number of high transaction weighted utility item sets in first phase it causes performance degradation in terms of execution time and space requirement. Huge number of transaction weighted utilities in first phase also affect the second phase algorithm. Since more are high transaction weighted utilities itemset are generated. Huge number of generated high utility transaction weighted utilities is a critical issue when we talk about the performance of the algorithm.

E. HUI-Miner Algorithm

Liu et al. [3] in their work proposed a new algorithm along with a new data structure. Utility-list data structure is used in this algorithm. Algorithm is HUI-Miner algorithm for the discovering high utility pattern. The utility-list of an itemset stores its exact utility as well as an upper bound on the expected utility values of its supersets by using the remaining utility values stored in the list. The items are sorted and processed in the ascending order of transaction utility. The algorithm avoids the candidate verification and generation cost of itemset. On the other side the utility joining operation is very costly and hampers the overall performance of the algorithm.

F. Fp Growth Algorithm

J. Han et al. [5] proposed a novel method for the same aim of discovering the high utility pattern from the data bases. Frequent pattern tree (FP-tree) structure was proposed; FP- tree structure as an extended prefix tree structure for storing crucial information about frequent patterns into compressed structure proposed an extended prefix tree structure of frequent pattern tree. And also developed an efficient FP-tree based mining method that is frequent pattern were mined by the pattern fragment growth using the FP-Growth. In it, a new highly compact FP-tree are constructed, which is usually smaller than the original databases, since the databases scan cost is minimize in the subsequent mining process. It reduces cost of candidate’s generation by applying growth method. But FP Growth algorithm consume more memory and performs badly with long pattern dataset and therefore not able to find high utility patterns.

IV. Proposed Work

A new algorithm has been proposed for discovering high utility patterns in single phase association rule mining which uses parameters such as statistical threshold-based pruning. Pruning is used here for reducing the memory and time required for mining high utility item sets.

Discovery high utility patterns from a dataset is done by setting a threshold value which is often derived through several runs or experiments with the algorithm. If Utility of any itemset is less than minimum threshold utility than that itemset will be an uninteresting pattern. For finding high utility item sets we can follow these steps:

*a)*First the algorithm takes transaction dataset, External Utility value and Minimum threshold value. After that database projection is performed on the itemset and at last identical transaction are merge. Each projection database taking only a linear time.

*b)*Two upper bound methods are then applied on utility value.

*c)*The upper bound is calculates and finally high utility item sets are mined.

V. Result Analysis

Testing has been done on the applied on the datasets as defined previously. Testing has been done on the two dataset and results are shows in which comparison is presents in terms of Memory requirement, Time requirement and number of Overlapped Patterns. The proposed and existing algorithm have been evaluated on two different samples. The graph has been plotted after testing on the different number of samples of datasets with different minimum support for Apriori Algorithm and minimum threshold for proposed algorithm. The above graph Fig.1 has been shown

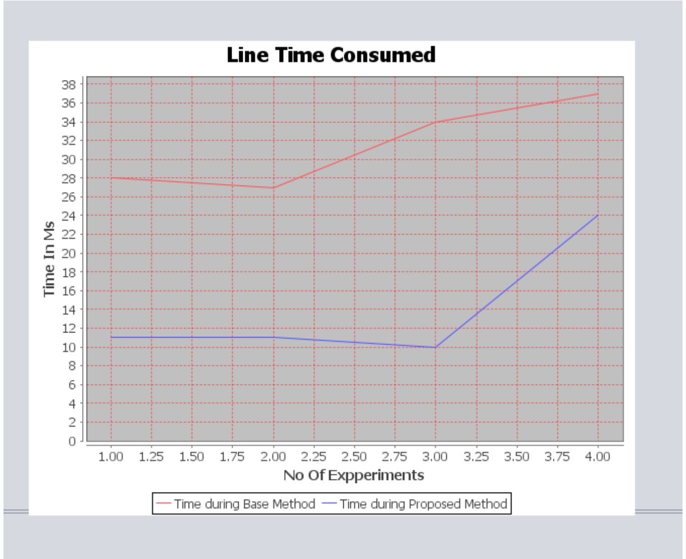


Fig. 1. Graph for Time

between ’Time’ and ’Number of Experiment’. Number of experiments represents the number of folds taken during bagging. Here ’4’ has been taken as number of folds. For the given number of folds time required for the proposed algorithm is less than the time required for based algorithm. It reduces time complexity in the proposed algorithm, and improve performance. The above graph Fig. has been shown between ’Memory’ and ’Number of Experiment’. Number of experiments represents the number of folds taken during bagging. Here ’4’ has been taken as number of folds. For the given number of folds memory requirement for the proposed algorithm is less than the time required for based algorithm. It reduces space complexity in the proposed algorithm, and improve performance. The above graph Fig.3 has been shown between ’Number of overlapped patterns’ and ’Number of Experiment’. Number of experiments represents the number of folds taken during bagging. Here ’4’ has been taken as

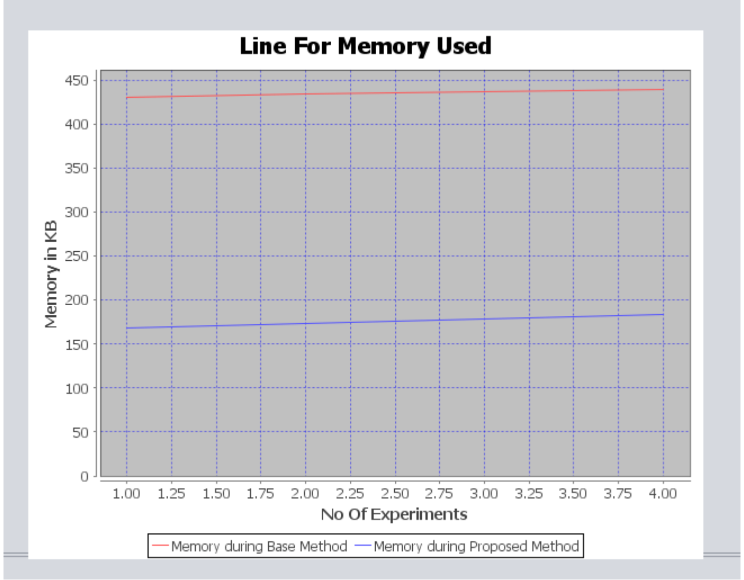


Figure 2. Graph of Memory

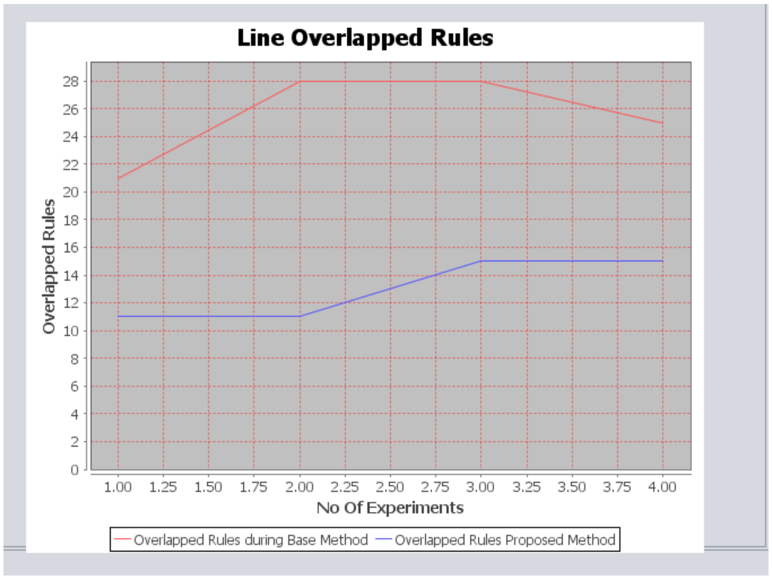


Fig. 3. Graph for Number of overlapped patterns

number of folds. For the given number of folds number of overlapped patterns for the proposed algorithm is less than the time required for based algorithm. It also improves performance of the algorithm.

VI. Conclusion

In data mining, utility mining is a new approach in which mining results must meet user's goals. Existing algorithms of association rule mining do not consider interestingness measures for users. Previously many algorithms were pro- posed for frequent pattern mining, but most of them mainly based on the count or occurrence value of an itemset. In this project, a new approach for high utility pattern mining has been proposed which uses pruning and bagging methods to improve performance. Pruning has been used on minimum threshold value to reduce candidates item sets while sampling with replacement using bagging method has been used to find best results. The proposed approach performs better in discovering the high utility patterns, it is shown in the experiments results, however memory required is sometimes depending on samples. As the proposed approach uses pruning for eliminating uninteresting patterns for reducing the time and memory required, it reduces the time but for different sample memory requirement may change.

VII. Future Work

In this project, high utility patterns are mined to presents appropriate results to a User. Future work may focus on the changing memory requirement with the changing samples. Another is which can be of interest may be secured utility mining.

References

[1]. R. Agrawal and R. Srikant, "Fast algorithms for mining association rules," in Proc. 20th Int. Conf.Very Large Databases, pp. 487–499,1994.

[2]. Y. Liu, W. Liao, and A. Choudhary, "A Two-Phase Algorithm for Fast Discovery of High Utility Itemsets" in Pro Conference on Knowledge Discovery and Data Mining, pp. 253–262, 2005.

[3]. M. Liu and J. Qu, "Mining high utility Itemsets without candidate generation" IEEE Trans. Knowl. Data Eng., vol.28, pp. 55 –64, 2012.

[4]. Y.-C. Li, J.-S. Yeh, and C.-C. Chang, "Isolated Items Discarding Strategy for Discovering High Utility Itemsets," Data and Knowledge Eng., vol. 64, no. 1, pp. 198-217, Jan. 2008.

[5]. J. Han, J. Pei, and Y. Yin, "Mining frequent patterns without candidate generation," Proc. ACM SIGMOD Int. Conf. Manage. Data, pp. 1 –12, 2000.

[6]. L. Geng and H. J. Hamilton, "Interestingness measures for data mining: A survey", ACM Comput. Surveys, vol. 38, no. 3, p. 9, 2006.

[7]. H. Yao, H. J. Hamilton, and L. Geng, "A unified framework for utility-based measures for Mining Itemsets," Proc. ACMSIGKDD 2nd Workshop Utility-Based Data Mining, pp. 28 –37, 2006,

[8]. J. Han and Y. Fu, "Discovery of Multiple-Level Association Rules from Large Databases," Proc. 21th Intl Conf. Very Large Data Bases, pp. 420-431, Sept. 1995.

[9]. C. F. Ahmed, S. K. Tanbeer,B. S. Jeong, and Young-Koo Lee "Efficient Tree Structures for High Utility Pattern Mining in Incre- mental Databases," IEEE Trans. on Knowl. and Data

Engineering, VOL NO. 12, DECEMBER 2009 pp. 1708-1721, Sept. 1995.

[10]. V. S. Tseng, B.-E. Shie, C.-W. Wu, and P. S. Yu, “Efficient algorithms for mining high Utility itemsets from transactional databases,” IEEE Trans. On Knowl. and Data Engineering, VOL. 25, NO.8 pp. 1772- 1786, Aug. 2013.

Low Power CMOS Op-amp with Optimized Settling Time

[1*]Dr. U.B.S. Chandrawat
[1*]Department of Electronics Communication Engineering
Acropolis Institute of Technology & Research India
[*]ucchandrawat@acropolis.in

Abstract

This paper presents a design of fast settling CMOS operational amplifier with a view to optimize the power consumption. Proposed method is based on keeping appropriate spacing between poles and zero so an underdamped transient response with minimum settling time can be obtained with less power consumption. Mathematical analysis using device modeling has been done to determine element values for optimum compensation followed by its simulations in triple metal layer n-well CMOS process using 0.5 μ technology. Best simulation results obtained on Tanner tool show 86.2dB gain, 136.6 MHZ Unity gain frequency(ω_u), 25 ns Settling time (t_s) with 1pf load, 211V/us Slew rate (SR) with 1pf load, and 2.56mW of power dissipation.

Keyword: CMOS, Op-amp, Power consumption, Settling time

I. Introduction

Fast settling and high slew rate are the key design parameters of a wide bandwidth fast settling operational amplifier. Many aspects of the settling behavior and frequency response of operational amplifiers (opamps) have been analyzed by various authors [1][2][3][4]]. The settling time consists of two distinct periods [2] the first one is the slewing period resulting from the limited available current of the input stage to charge the compensation capacitor. During this period, the amplifier acts in nonlinear fashion and the output makes the transition from the initial value to the vicinity of the new value. In the second period after the slewing period, amplifier starts to settle to the final value in a quasi linear fashion. To reduce the settling time of operational amplifier standard circuit approaches such as input stage transconductance reduction [4], doublet compression [3], and optimum phase margin [1] have been found in literature. Input stage transconductance reduction has shown with low tranconductance at input stage of two stage opamp better settling time can be obtained. In doublet compression effect of frequency doublets on settling time has been discussed, and it has been concluded that the frequency doublets (pole-zero pair) in the transfer function of an operational amplifier may cause severe degradation in settling time. A reduction of spacing between pole and zero can minimize effect of doublets. In optimum phase margin relationship between phase margin and settling time has been discussed and concluded that best settling time can be obtained at specific phase margin.

Little has been done for getting optimum value of other parameters (power, size etc.) with minimum settling time of operational amplifier. It is well known that when amplifier starts to settle in the quasi linear region (second period of settling time), the output may be under-damped, over damped or critically damped depending on circuit parameters as shown in Fig.1. In quasi-linear region, minimum-settling time can be obtained when the Op-amp is under-damped and the location of non-dominating frequency with respect to dominating frequency chosen such that the first peak of the step response just touches the upper settling error limit. To minimize the settling time right-half-plane zero is assumed to be at very high frequency relative to the unity gain frequency[1].

When compensation element values calculated as per [1] designed Op-amp is achieving good settling time but consume more power.

II. Theory of operation

Operational amplifier can be well approximated by a two-stage configuration i.e. differential stage followed by a gain stage. as shown in Fig. 3 .The unity gain close loop transfer function, A(s), is given as:

$$\mathrm{A}(\mathrm{s}) = \frac{A(o)}{\left(s/\omega o\right)^{2} + 2k\left(s/\omega o\right) + 1} \qquad (1)$$

here $A(o) = \frac{a(o)}{1+a(o)}$, $\omega o = \left[\omega 1 \omega 2 (1+\mathrm{ao})\right]^{1/2}$

damping factor $\mathrm{k} = \frac{\omega 1 + \omega 2}{2\,\omega o}$, a (o) is the low frequency gain of the opamp and ω_1 and ω_2 are the radian frequencies of the first and second left half plane poles respectively. The pole separation factor $\beta = \omega_2/\omega_1$, Damping factor k in terms of pole separation factor can be given as

$$\mathrm{k} = \frac{1+\beta}{2\left[\beta\left(1+a_{O}\right)\right]^{1/2}} \qquad (2)$$

The second order transfer function given by (1) has three possible responses to a voltage step input; namely over damped (k>1), under damped (k<1), critically damped (k=1). When the opamp is under damped and the first peak of the step response just touches the upper settling error limit minimum settling time can be obtained [2] so we will consider only case of k<1 and apply inverse Laplace transform to (1), so normalized time response can be expressed as:

$$\mathrm{vo} = 1 - \left\{ \begin{matrix} \left\{ k/\left(1-k^{2}\right)^{1/2} \sin\left[\left(1-\mathrm{k}^{2}\right)^{1/2} \omega_{o} t\right] \right. \\ \left. + \cos\left[\left(1-\mathrm{k}^{2}\right)^{1/2} \omega_{o} t\right] \right. \end{matrix} \right\} \exp(-k\omega o t) \qquad (3)$$

As a first step in finding the shortest response time of the second order system, the time of the first peak of the under damped response, t_p is determine by setting the first derivative of (3) equal to zero.

$$\mathrm{tp} = \frac{\pi}{\omega o\left(1-\mathrm{k}^{2}\right)^{1/2}} \qquad (4)$$

Now error tolerance voltage is considered as D and input step applied is 1 volt then 1+D would be the value of first peak for minimum settling time. The normalized voltage of the first peak determined by using (3) and (4) and is equal to one plus the overshoot:

So,

$$\text{First peak} = 1 + \exp\left[\frac{-k\pi}{\left(1-k^2\right)^{1/2}}\right]$$

$$D = \exp\left[\frac{-k\pi}{\left(1-k^2\right)^{1/2}}\right] \qquad (5)$$

By using (2) and (5) with β>>1 the optimum pole separation factor βo can be determined as

$$\beta_o = \frac{4\left(1+a_o\right)}{1+\left(\pi/\ln D\right)^2} \qquad (6)$$

From two pole small- signal equivalent circuit of a two-stage opamp pole and zero can be given by

$$\omega 1 = \frac{g_1 g_2}{\left(gm_2 + g_1 + g_2\right)C_C + g_2 C1 + g_1 C2} \quad (7)$$

$$\omega 2 = \frac{\left(gm_2 + g_1 + g_2\right)C_C + g_2 C1 + g_1 C2}{C1C_C + C2C_C + C1C2} \quad (8) \qquad \omega_Z = \frac{1}{C_c\left(1/gm_2 - R_C\right)} \quad (9)$$

$\omega u\left(UGF\right) = \frac{g_{m1}}{C_C}$, Where ω_1, ω_2 are pole frequencies, ω_z is zero frequency, g_{m1} is the transconductance of the first stage, g_{m2} is the transconductance of the second stage,C_c is compensation capacitor and R_c is compensation resistance.

Conventionally zero frequency is used to cancel pole frequency or placed at very high frequency so it can be neglected. But our analysis has shown that if zero frequency placed at appropriate distance away from unity gain frequency for particular capacitive load, then best settling time can be obtained with reasonable low power consumption. Using simulation tool by varying compensation elements one can place zero at different locations near to unity gain frequency and it is found that for different capacitive load best settling time can be obtained only at appropriate location of zero frequency with respect to unity gain frequency. Table 2 shows settling time for different locations of zero frequency for 1pf capacitive load. It is found that the best settling time can be obtained when zero frequency is 1.377 times of unity gain frequency, so for getting optimum values of compensation elements we consider

$$\omega_Z = 1.377\,\omega_\mu \qquad 10)$$

$$\omega 2 = \omega 1 \beta_o \qquad (11)$$

By using equations from 7to11we can get values of Rc and Cc as:

$$C_C = \frac{4(1+a_o)(C1+C2)}{1+(\pi/\ln D)^2 (gm_2)^2} \tag{12}$$

$$R_C = \frac{1+\left(\pi/\ln D\right)^2 (g_{m2})}{5.5\,\omega u\,(1+a_o)} \tag{13}$$

III. Design Implementation

Specification targeted are settling time 25ns, power dissipation 5mW, Gain 80db, bandwidth 5 MHz. By using triple metal layer n-well 0.5μ CMOS process two stage miller CMOS opamp (Fig.2) has been implemented. Specification taken as bench mark are**:** open loop dc gain (Ao)=90db, UGB(ω_μ)=150MHZ, slew rate(SR)= 250 v/μs (for 1pf load), power dissipation = 2.5 mW. Driving voltage (veff.) of M_1, M_2 assumed equal to 0.45volt (v) so a high slew rate can be achieved. Reasonable value of input common mode range (ICMR) can be obtained by assuming driving voltages (veff.) of M_3, M4, M5 equal to 0.2v and for high output swing veff.of M_6, M7 will be kept equal to0.2v.We will assume Cc=0.2pf and find out I_1 from relationship $SR = \frac{I_1}{Cc}$. To keep power dissipation equal to 2.5mW maximum possible value of I_2 can be find out as power dissipation = $\left(I_1 + I_2 + \frac{I_1}{2}\right)V_{dd}$. By using value of I_2 we can find out g_{m7} as $g_{m7} = \frac{2I2}{veff}$. Computed value of g_{m7} and D (0.1 % value of steady state value of out put voltage) used to find out Cc and Rc from (12) and (13) respectively. As current I_1 and I_2 is known to us and V_{eff} we have assumed, Width/Length (W/L) ratio of different transistors in Fig.2 can be find out by using given relationship.

$$\frac{W}{L} = \frac{2Id}{k'\,Veff.^2} \tag{14}$$

Where I_d is the drain current flows through different transistors, k' is process gain factor and is equal to $\frac{\mu_n C_{ox}}{2}$. Minimum possible length of transistors can be kept 0.5μ but to avoid second order effects such as channel length modulation we consider L=1.5μ. So Width (W) of the transistor can be find out from (14). For two-stage CMOS opamp (Fig.2) Open loop dc gain (A_o) can be given as

$$A_o = g_{m1} g_{m7} \left(r_{o2} \| r_{o4}\right)\left(r_{o7} \| r_{o8}\right) \tag{15}$$

Where $r_{o2}, r_{o4}, r_{o7}, r_{o8}$ are dynamic resistance of MOS transistor and can be given as $ro = \frac{1}{\lambda\, Id}$, λ is channel length modulation parameter and is equal to $\frac{\partial V_{DS} / \partial I_{DS}}{I_{DS}}$. Here V_{DS} = voltage across drain and source and I_{DS}=current flowing between drain and source, Id is drain current flowing through MOS transistor. λ is technology dependant parameter and its value for 1.5u length of transistor generally assumed equal to $0.03\,v^{-1}$.By using this value of λ and calculated values of $g_{m1}g_{m7}$ we can find open loop dc gain from(15).

IV. Result and Discussion

The design strategy presented in this paper is focused on obtaining a controlled transient response of a two stage miller operational amplifier as shown in Fig.1. If opamp is compensated with the help of derived values of R_c and C_c given by (12) (13) then a fast settling time can be obtained for required error tolerance voltage (D) and transconductance of second stage (that will influence power dissipation). It has been reported in literature [1] that minimum settling time can be obtained at specific phase margin in the vicinity of 70°. When the design strategy given by [1] is used for designing of a two stage miller CMOS opamp, simulation result shows fast settling time while power consumption is found up to 5mW.Reason of high power consumption is due to traditional method of obtaining optimum phase margin (in the vicinity of 70°) in which zero should be placed at very high value, and non-dominating frequency should be placed at two to three times of unity gain frequency. Higher non-dominating frequency is obtained by keeping high value of transconductance of second stage, which requires hundreds of microamperes current through second stage that is responsible for high power consumption. With the design strategy presented in this paper, power dissipation is reduced to 2.5mW. As per given design strategy there is no need to place non-dominating frequency at very high value. By keeping zero frequency at a specific distance from unity gain frequency for specific load capacitor we can get optimum phase margin even if non-dominating frequency remains at a distance 1.5 times of unity gain frequency. Our work is applicable only for the on chip operational amplifiers due to higher impedance of second stage, so only low value of capacitive load can be used. Same work can be extended for variable capacitive and resistive load by adding buffers as an output stage. The values of derived compensation resistor will provide minimum settling time for specific capacitive load (for 1pf capacitive load in given design). If capacitive load is required to be kept equal to 0.5 pf then derivation of value of the compensation resistor must be done by using ω_z=1.12 ω_u instead of relationship given by (10) (refer Table 1 and Table 2).

Table l: Settling time for different location of zero frequency relative to unity gain frequency at capacitive load of 1pf.

Compensation Resistor (Rc)	**Location of zero freq.**	**Settling time**
3.58kΩ	$\omega z = 1.59\ \omega\mu$	27.82 ns
3.65kΩ	$\omega z = 1.52\ \omega\mu$	27.60 ns
3.95kΩ	$\omega z = 1.44\ \omega\mu$	27.34 ns
4.14kΩ	$\boldsymbol{\omega z = 1.37\ \omega\mu}$	**27.12 ns**

4.32kΩ	ωz = 1.26 ωμ	27.39 ns
4.52kΩ	ωz = 1.21 ωμ	27.47 ns
4.69kΩ	ωz = 1.16 ωμ	27.46 ns

Table 2: Settling time for different location of zero frequency relative to unity gain frequency at capacitive load of 0.5pf.

compensation resistor (Rc)	**location of zero freq.**	**Settling time**
3.95kΩ	ωz =1.44 ωμ	21.00 ns
4.14kΩ	ωz =1.37 ωμ	20.77 ns
4.32kΩ	ωz =1.26 ωμ	20.59 ns
4.52kΩ	ωz =1.21 ωμ	20.39 ns
4.69kΩ	ωz =1.16 ωμ	20.01 ns
4.95 kΩ	**ωz =1.12 ωμ**	**19.64 ns**
5.20 kΩ	ωz = 1.08 ωμ	19.84 ns

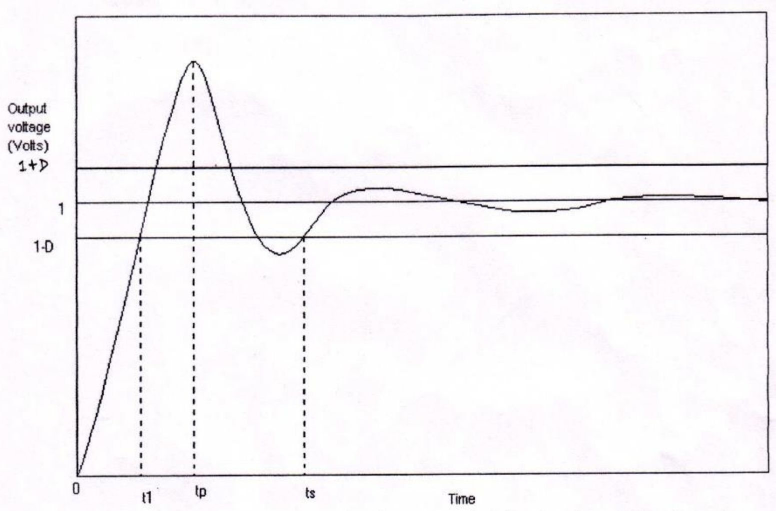


Figure 1. Underdamped response of second order system when damping factor is less then unity

Where

t_p = Time of first peak of the underdamped response. D = Error tolerance voltage.

t_1 to t_s= Quasi-Linear region i.e. second Period of settling time. t_s = Settling time.

t_1 = Slewing time i.e. first Period of settling time.

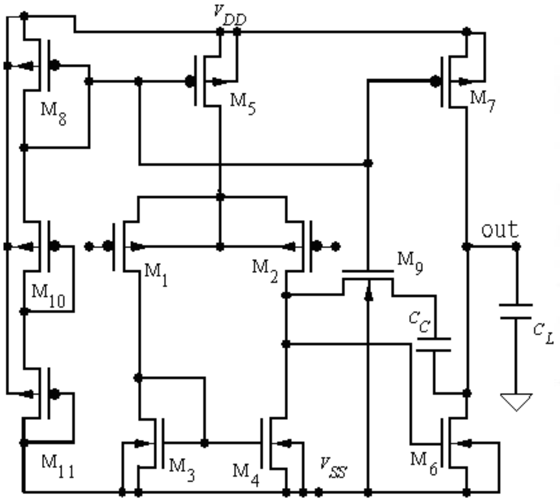


Figure 2.Two-stage CMOS opamp with biasing circuit

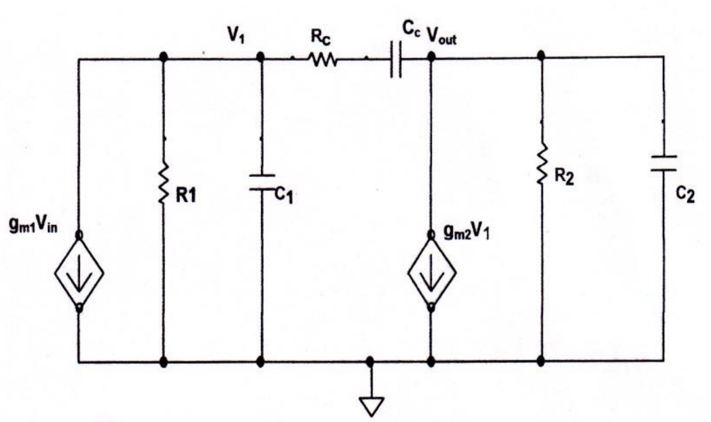


Figure 3. Small signal model of two pole opamp with compensation capacitor and resistor.

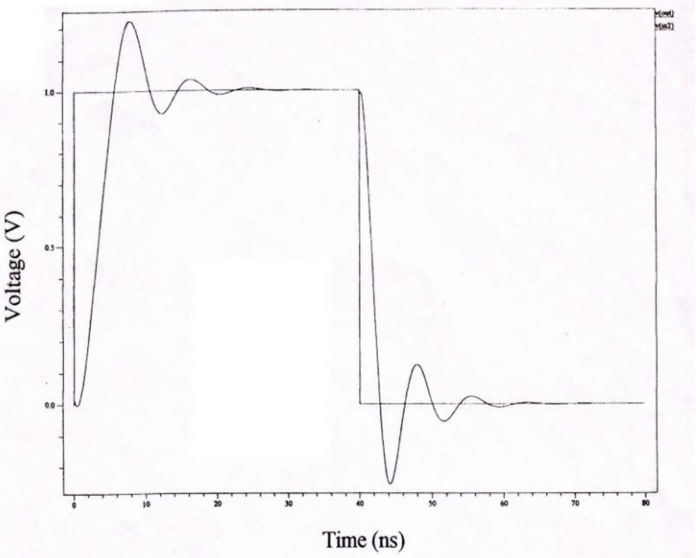


Figure 4. Settling performance of designed CMOS opamp

References

[1]. Devid A. Johns and Ken Martin Analog Integrated Circuit Design, John wiley & Sons, Inc. 1997.

[2]. Allen P. Holberg D.,CMOS Analog Circuit Design, Holt Rinehart and Winston Inc. 1987.

[3]. B. Y. Kamath, R. G. Meyer, and P. R. Gray, “Relationship between frequency response and settling time of operational amplifiers”, *IEEE J. Solid-State Circuits*, vol. SC-9, pp. 347-352, Dec.1974.

[4]. R.J. apfel and P.R. Gray, “A fast settling monolithic opamp using doublet compression techniques” IEEE J. Solid-State circuits vol. SC-9, pp.332 - 340, Dec. 1974

Script Recognition Methodology: A Survey
A Theoretical study of recognition techniques

[1*]Gamini Bhoi, [2]Prashant Richhariya
[1*]Computer Science & Engineering
Chhatrapati Shivaji Institute of Technology India
[2]Computer Science & Engineering
Indore Institute of Science and Technology India

[1]bhoigamini27@gmail.com , [2]prashant1579@gmail.com

Abstract

Script recognition is one of the interesting and challenging fields of pattern recognition. Script is defined as the graphic form of the writing system used to write statements expressible in language. The nee of script recognition algorithm is due to the increasing demand of paperless world. There are number of different scripts used in different languages including Devanagari, Gurumukhi, etc. hence script recognition is essential for recognizing the character written in different script. For this various methodology and algorithm are developed which is discussed here. There are several methods developed so far for script recognition. This survey is the study of script can be recognized online as well as offline. Offline script recognition mainly focuses on handwritten documents. [17]

Key-Words- OCR (Optical Character recognition), Online recognition, Offline recognition, Convolution neural network, Dynamic time warping, Deep learning,

I. Introduction

Humans can easily recognize, read and interpret the characters word by word, letter by letter that what is written in front of them. Sometimes when the handwriting is not so good then also our brain recognize it because our brain is that much trained or developed that it can easily analyze what may be the word is, if it is not able to recognize then it manages itself that what may be come in this place or it is resembling to which word. All in all humans can also read bad handwriting with more than 90% accuracy. This recognition gives a significant benefit in order to bridge the gap between man and machine communication. [1] What makes it possible is the Artificial Intelligence, Deep Learning etc. OCR or Optical Character Recognition is a traditional method of script recognition. It is working very smartly, although previously it was not so smart in working. The day by day developments in the computer make it so good that now it can easily read your handwriting and recognizes it. OCR fonts are developed in which there were standard fonts and for recognition process only these fonts were followed. The OCR standard fonts are shown below:-

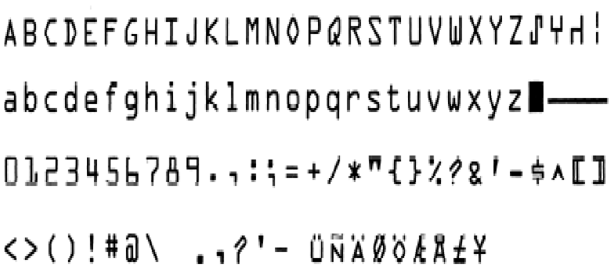
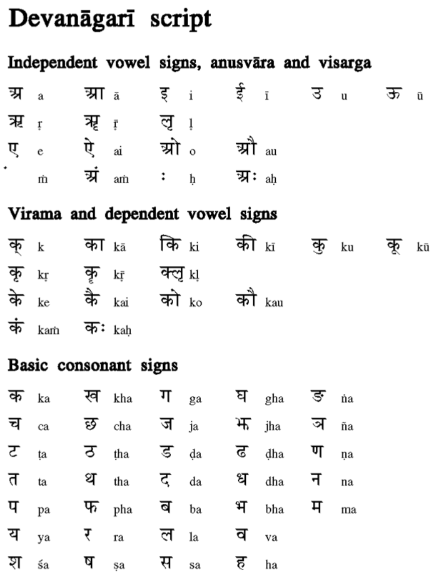


Fig1. OCR standard fonts

After that the features expanded and now the commonly used fonts like Times New Roman, Arial started using so that the system can also recognize these fonts but again the person can write in any style, so the next system which were developed is the concept where the scripts are broken into smaller parts so that the characters are recognized and then the complete word by word. This smart learning of computers is what we called as Deep Learning,[14][15] a concept of AI. It is also able to analyze what the next word should come grammatically.
For example: - you must have seen in your smart phones whenever you type something you come up with the suggestion of next word. Similarly Google translate app translates a word or sentence on the spot as soon as you scan it.

Fig 2 Google Translate

So we can see that according to the changed scenario script recognition methodologies are also changing , capabilities are improving, even we can take feedback also whose application is the use of captcha code. Devnagiri script is one of the important script used in India. It is used to write Hindi, Sanskrit, Marathi etc. For Devnagiri script recognition the input is preprocessed and segmented followed by extraction and classification. [20] There are number of researches have been done in script recognition such as offline handwritten English script recognition[4] ,online handwritten script recognition[1], about Indian scripts:- Devnagiri, Bangla, Tamil, Oriya etc. [5] [16]The main function of script recognition is to classify it into one of the available script which include English, Chinese, German, Arabic etc. [6]The main objective of the handwritten character recognition is to effectively extract the features of the script so that the further processes work successfully. [7]



Devanāgarī script

Independent vowel signs, anusvāra and visarga

अ	a	आ	ā	इ	i	ई	ī	उ	u	ऊ	ū
ऋ	ṛ	ॠ	ṝ	ऌ	ḷ						
ए	e	ऐ	ai	ओ	o	औ	au				
ं	ṁ	अं	aṁ	ः	ḥ	अः	aḥ				

Virama and dependent vowel signs

क्	k	का	kā	कि	ki	की	kī	कु	ku	कू	kū
कृ	kṛ	कॄ	kṝ	क्लृ	kḷ						
के	ke	कै	kai	को	ko	कौ	kau				
कं	kaṁ	कः	kaḥ								

Basic consonant signs

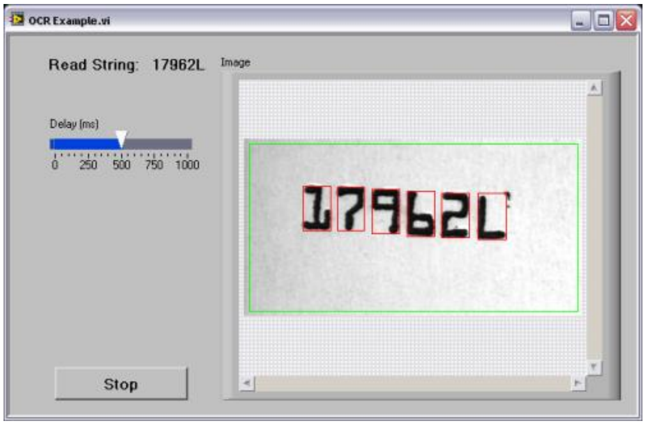
क	ka	ख	kha	ग	ga	घ	gha	ङ	ṅa
च	ca	छ	cha	ज	ja	झ	jha	ञ	ña
ट	ṭa	ठ	ṭha	ड	ḍa	ढ	ḍha	ण	ṇa
त	ta	थ	tha	द	da	ध	dha	न	na
प	pa	फ	pha	ब	ba	भ	bha	म	ma
य	ya	र	ra	ल	la	व	va		
श	śa	ष	ṣa	स	sa	ह	ha		

Fig 3 Devnagari Script

1. Literature Review

With the development of AI, machine learning and deep learning lots of algorithms are also developed for script recognition which reduces the time and efforts with their accuracy and reliable nature. Working of some of the algorithms are discussed here.OCR is a mechanism for recognition of handwritten text; printed text etc or we can say that OCR is a mechanism/technology that converts printed text into digital format. The basic steps of OCR for script recognition are: Preprocessing: This is the fundamental steps of OCR where the input is preprocessed, noises are removed, and then the image is binarize (black and white).The next step is feature extraction and finally recognition. Feature Extraction: This algorithm interprets the character, reduces it into smaller dimension. Pattern Recognition: Identifying a character as a whole with the use of distance formula

$$d= \sqrt{} (y_2- y_1)^2- (x_2- x_1)^2$$



Read String: 17962L

Fig 4 An OCR example

The writing in different fonts makes it difficult to recognize a text. The character recognition is of two types printed and handwritten. Handwritten character recognition is again divided into two categories online and offline recognition. [1] Online documents can be generated with the help of tablet PCs, laptop using different scripts and fonts. [2] Offline handwritten character recognition includes the automatic conversion of text into an image. Offline character recognition is tougher than online recognition. [3] [12]Offline handwriting recognition is the task of determining what letters or words are present in a digital image of handwritten text. [18] Handwritten text such as English cursive script is recognized using following steps. At first the system is trained with a cursive image as an input and it is converted into a grey scale image than an adaptive thresholding [19] process is applied for binarized image. This image is extracted by eliminating unwanted lines between characters followed by classification. Convolution Neural Network algorithm starts with an example that how a kid learns the things. A kid learns everything on the basis of training provided by his mother, family and environment, he is trained with the alphabets by making him learn and memorize it so that the next time if he asked to identify the character he must be able to identify that character. It may be a script, image, video, objects or a person in the place of character. If he is not able to remember then by trial and error method anyhow he will be able to recognize it. In the same way convolution neural network works. There are number of neural networks present here just like neurons in the human brain which helps it to recognize the script. The first step is to train the networks with input datasets and an appropriate output and then hidden layers process this input, matches it with the patterns and gives an appropriate output. The image below describes the working of convolution neural network.

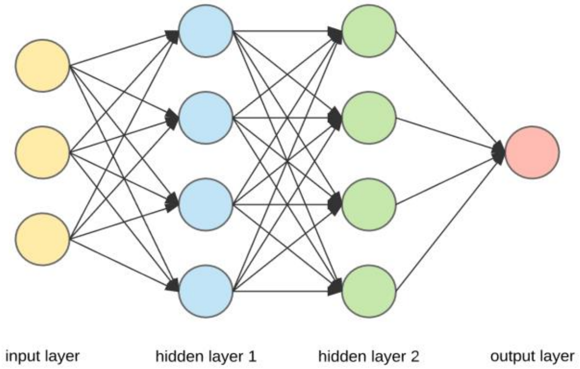


Fig 5 Convolution Neural Network

The high variability in the script styles is the major difficulty of script recognition. The method which is invariant to scale and rotation is based on the DTW (Dynamic Time Warping) algorithm. DTW is used for matching the distances and K-nearest neighbor algorithm is used as classifier [9], [10] the minimum distance between the drawn character and the original character is the result of recognition. DTW algorithm is used for both single stroke[13] and multi stroke handwritten characters. [11]The other method of script recognition is a Scikit learn, it is a python package of machine learning. It consists of inbuilt implementation of machine learning concept such as linear regression, decision tree to make it more efficient. With this we can use the fraction of classification, regression, clustering. [8]

2. Result Discussions

The number of researches done in the field of script recognition is already describing the importance of pattern recognition. Despite all the methodologies discussed here many more to come such as incorporation of different scripts in different handheld devices like mobile, tablet, tabletop systems etc, particularly for those who previously felt that script recognition is not in their reach. Further empirical analysis can help in the choices of algorithms which will be chosen on the basis of accuracy they provide.

3. Conclusion

Script Recognition has been around for a long time, however as of late has turned into a rising innovation. When I look back on different methodologies, algorithms and research work done in the field of script recognition, I come to the conclusion that any type of script recognition requires the following mains steps i.e. preprocessing, feature extraction any final recognition. Script recognition is such a complex task. This is somehow made easy with the available of pre-prepared datasets, with these datasets the algorithms can be trained so good that it works with more and more accuracy.

Acknowledgment

To discover, analyze and to present something new is to venture on an unknown path towards an unexplored destination unless one gets a true torch bearer to show the way. I express my sincere gratitude to my guide,**Mr. Prashant Richhariya** for his valuable guidance and support for the successful completion of the work.

References

[1]. Manish K., M.K Jindal and R.K Sharma, Review on OCR for Handwritten Indian Scripts character recognition.

[2]. Anoop M. Namboodiri and Anil K. Jain, On- line Script Recognition.

[3]. Karishma P., M. Gandhi, Offline Handwritten Character Recognition: A Review, International journal of scientific and research, vol.7, issue 5. 2016.

[4]. Dhaka V. S., M. Kumar, P. Chaudhary, Offline Handwritten English Script Recognition: A survey, Special Confernece Issue: National Conference on Cloud Computing and Big Data.

[5]. Pal U., Indian script character recognition: a survey, 2004

[6]. Bhunia A. K., A. Konwer, A. Bhowmick, P. P. Roy, U. Pal, Script Recognition in Natural Scene Image and Video Frame using attention-based convolution LSTM network.

[7]. Fornes A., J. Llados, G. Sanchez, D. Karatzas, *Rotation Invariant Hand Drawn Symbol Recognition based on a Dynamic Time Warping Model.*

[8]. www.google.com

[9]. Roy S., M. Saravanan, *Handwritten Character Recognition using K-NN classification algorithm*, IJARIIE-ISSN (0)-2395-4395 Vol. 3 Issue-5, 2017.

[10]. Ong V., D. Suhartono, *Using K-Nearest Neighbor in Optical Character recognition,* camtech vol 7. Issue. no. 1. 53-65. 2016.

[11]. Mouchere H., J. li, C. Viard- Gaudin, Z. Chen, *A Dynamic Tie Warping Algorithm for Recognition of Multi- Stroke On –Line Hnadwritten Characters*. Natural Science Editon, Journal of South China University of Technology, 41 (7). pp. 107-113. 2013.

[12]. Sridhar P., *Online Hand Writing Recognition System on Android Based Mobiles*. International Journal of Science and Technology, Vol.5 (4). 5729-5733. 2014.

[13]. Neo C. C., E. Lee Ming Su, P. I. Khalid, C. Fai Yeong, *Method to Determine Handwriting Stroke Types and Directions for Early Detection of Handwriting Difficulty*, International Symposium on Robotics and Intelligent Sensors 2012 (IRIS).2012.

[14]. Shubham S. M., S. Solanki, S. Gupta, S. Dhingra, M. Jain, R. Saxena, *Handwritten Text Recognition: with Deep Learning and Android.* International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8, Issue-3S, February 2019

[15]. Balci B., D. Saadati, D. Shiferaw, *Handwritten Text Recognition using Deep Learning*.

[16]. Sujatha P., D. Lalitha Bhaskari, *Telugu and Hindi Script Recognition using Deep learning Techniques*, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol-8, Issue-11, September 2019

[17]. Ghosh D., T. Dube and A.P. Shivaprasad, *Script recognition-A Review*. IEEE transactions on pattern analysis and machine intelligence, Volume XX, No- YY, month 2009

[18]. Mukund Y. P., M. S. Deshpande. *English Cursive Script Recognition*. International Journal of Engineering Sciences and Research Technology, ISSN: 2277-9655

[19]. Shafait F. et al., Efficient Implementation of Local Adaptive Thresholding Techniques Using Integral Images, in Document recognition, 2007.

[20]. Aradhna A Malankar, M. M. Patel, *Handwritten Devnagari Script Recognition: A Survey*. IOSR Journal of Electrical and Electronics Engineering(IOSR- JEEE) e- ISSN: 2278-1676, Volume 9, Issue 2 Ver.II (Mar- Apr. 2014), PP 80-87